AUDIT OF THE DEPARTMENT OF JUSTICE'S IMPLEMENTATION OF AND COMPLIANCE WITH CERTAIN CLASSIFICATION REQUIREMENTS

U.S. Department of Justice
Office of the Inspector General
Audit Division

Audit Report 13-40
September 2013

AUDIT OF THE DEPARTMENT OF JUSTICE'S IMPLEMENTATION OF AND COMPLIANCE WITH CERTAIN CLASSIFICATION REQUIREMENTS

EXECUTIVE SUMMARY

In 2010, Congress passed Public Law 111-258, the *Reducing Over-Classification Act* (Act), which, among other things, directed the Inspector General of certain federal agencies, including the Department of Justice (DOJ), to: (1) assess whether applicable classification policies, procedures, rules, and regulations have been adopted, followed, and are effectively administered within such department, agency, or component; and (2) identify policies, procedures, rules, regulations, or management practices that may be contributing to persistent misclassification of material within such department, agency, or component. The Act requires the evaluation to be completed by September 30, 2013. A second evaluation required by the Act, which is due by September 30, 2016, will review DOJ's progress in implementing the recommendations of this audit.

Background

The appropriate classification of information is critical to the government's efforts to ensure national security. However, the 9/11 Commission, Congress, and the White House have recognized that over-classification of information interferes with accurate and actionable information sharing, increases the cost of information security, and needlessly limits stakeholder and public access to information.[1]

When information is identified as posing a risk to national security, an official with "Original Classification Authority" (OCA) designates the information as classified, known as an original classification decision.[2] OCA officials convey their classification decisions by marking the original document (or source document) or, more often, by capturing the

[1] The National Archives and Records Administration's (NARA) Information Security Oversight Office developed the working definition of "over-classification" as the designation of information as classified when the information does not meet one or more of the standards for classification under section 1.1 of Executive Order (EO) 13526. In other words, over-classification is either treating unclassified information as if it were classified, or classifying information at a higher level of classification than is appropriate.

[2] According to EO 13526, original classification authority is delegated by the President and the Vice President and can be further delegated by an agency head or certain other officials designated with original classification authority.

classification decision in a security classification guide. Once an OCA official classifies information, that information may be paraphrased, extracted, or summarized, which is known as a derivative classification decision. A derivative classifier must observe and respect the original classification decision and carry forward to any newly created document the pertinent classification markings from the source document(s) or the security classification guide.

Within DOJ, the Security and Emergency Planning Staff (SEPS) is responsible for implementing DOJ's classification management program and ensuring DOJ's organizational compliance with classified national security information laws, regulations, directives, and other guidance, as appropriate.[3] In addition, the Federal Bureau of Investigation's (FBI) National Security Branch and the Drug Enforcement Administration's (DEA) Office of National Security Intelligence are members of the Intelligence Community and as such also are subject to the classification policies established by the Office of the Director of National Intelligence (ODNI). Finally, DOJ is required to establish and implement uniform security polices and operational procedures for the classification, safeguarding, and declassification of national security information.

Results in Brief

We found that DOJ has established classification policies and procedures, but has not effectively administered those policies and procedures to ensure that information is classified and disseminated appropriately. Although our review of a small sample of classified documents created during fiscal year (FY) 2012 did not find indications of widespread misclassification, we did identify deficiencies with the implementation of DOJ's classification program, including persistent misunderstanding and lack of knowledge of certain classification processes by officials within DOJ components.

Based on these findings, we believe that the types of discrepancies we identified and the causes of those discrepancies indicate that DOJ is susceptible to misclassification.

Specifically, we found several documents in which unclassified information was inappropriately identified as being classified. We also identified many documents that either did not contain required classification markings or contained incorrect classification markings. Some of these

[3] SEPS is a component of DOJ's Justice Management Division.

marking errors included missing, incomplete, or incorrect classification blocks, source references, portion markings, dissemination markings, and declassification instructions. DOJ component officials generally agreed with our findings that some information in certain documents should not have been classified and that the markings on many documents were not accurate.

In addition, we found that the National Security Division, Criminal Division, and the DEA incorrectly categorized many decisions to classify information as "original" classification decisions when these decisions actually were derivative classification decisions, as the classified information in the documents had been classified previously. The risk inherent in this practice is that individuals who inappropriately apply original decisions could apply these decisions inconsistently for the same types of information and information that should be treated similarly will be classified differently across programs. Also, this practice could result in classifiers believing that they could establish the classification levels, dissemination controls, or declassification dates of their choosing rather than the ones previously established by the actual original classification decision.

We found several factors that we believe contributed to DOJ components incorrectly classifying and marking documents, including weaknesses in DOJ's implementation classification standards, the limited distribution of automated tools designed to improve the classification and marking processes, and weaknesses in the application of security education and training programs.

Ensuring that information is classified and marked appropriately falls within SEPS's responsibilities for developing and managing DOJ policy for classified national security information. With nearly 60,000 personnel authorized to access and derivatively classify national security information, SEPS's responsibilities are significant. SEPS has developed oversight and review processes for classified national security information, as directed by EO 13526, which prescribes a uniform system for classifying, safeguarding, and declassifying national security information. But SEPS has encountered problems executing and overseeing those procedures, in part because of insufficient resources devoted to these responsibilities and weaknesses in infrastructure, training, and controls throughout DOJ.

To help improve DOJ's classification management program and implementation of classification procedures, we made 14 recommendations to SEPS. These recommendations include determining the classified infrastructure enhancements that are needed to successfully use and share appropriate types of classified information; enhancing DOJ's classification

training programs to ensure that all personnel are aware of policies, procedures, and requirements for classifying national security information; and improving oversight practices to ensure that all DOJ components are reporting accurate information in classification-related reports and are in compliance with all regulatory requirements.

AUDIT OF THE DEPARTMENT OF JUSTICE'S IMPLEMENTATION OF AND COMPLIANCE WITH CERTAIN CLASSIFICATION REQUIREMENTS

TABLE OF CONTENTS

This page intentionally left blank

INTRODUCTION

The appropriate classification of information is critical to the government's efforts to ensure national security. However, the 9/11 Commission, Congress, and the White House have recognized that the over-classification of information interferes with accurate and actionable information sharing, increases the cost of information security, and needlessly limits stakeholder and public access to information.[4] In 2010, Congress passed Public Law 111-258, the *Reducing Over-Classification Act*, requiring federal agencies that classify information to implement programs that enforce compliance with applicable laws, executive orders, and other authorities pertaining to the proper classification of information and use of classification markings.

Executive Order (EO) 13526, which is referred to in the *Reducing Over-Classification Act*, prescribes a uniform system for classifying, safeguarding, and declassifying national security information.[5] The National Archives and Records Administration's (NARA) Information Security Oversight Office is responsible for issuing directives for implementing EO 13526 to all government agencies that come into possession of classified information.[6] In turn, DOJ is required to establish and implement uniform security polices and operations procedures for the classification, safeguarding, and declassification of national security information within the Department. In addition, the Office of the Director of National Intelligence (ODNI) is responsible for issuing implementation directives to the Intelligence Community related to the protection of intelligence sources, methods, and activities.[7] Within the Department of Justice (DOJ), the Federal Bureau of Investigation's (FBI) National Security Branch and the Drug Enforcement Administration's (DEA) Office of National Security Intelligence are members of the Intelligence Community and therefore must

[4] The National Archives and Records Administration's (NARA) Information Security Oversight Office developed the working definition of "over-classification" as the designation of information as classified when the information does not meet one or more of the standards for classification under section 1.1 of EO 13526. In other words, over-classification is either treating unclassified information as if it were classified, or classifying it at a higher level of classification than is appropriate.

[5] EO 13526, *Classified National Security Information,* December 29, 2009.

[6] These directives are identified in the Federal Register as 32 CFR Part 2001 and 2003 Part V *Classified National Security Information*; Final Rule, June 28, 2010.

[7] ODNI issues Intelligence Community policies and directives to the Intelligence Community through the Intelligence Community Policy System as designated by EO 12333.

abide by ODNI guidelines and directives in addition to those promulgated by DOJ.

Classified Information

EO 13526 mandates that information should be considered for classification when its unauthorized disclosure could reasonably be expected to cause identifiable damage to national security.[8] Such national security information may be classified as Top Secret, Secret, or Confidential, as shown in Exhibit I-1.[9] EO 13526 specifies that if significant doubt exists about what level information should be classified at, the information should be classified at the lower level.

[8] Classified information is not the only information that is shielded from the public. For instance, unclassified information that is law enforcement sensitive, information that is subject to executive, deliberative, or attorney-client privilege, and personally identifiable information, may all be withheld from the public under appropriate circumstances.

[9] Classified information also may be identified as Sensitive Compartmented Information (SCI). SCI is also referred to as "codeword" information. SCI is not a classification level, but rather a requirement for formal access controls. SCI refers to information associated with certain intelligence sources, methods, or analytical processes. The sensitivity of SCI requires that it be protected in a much more controlled environment than other classified information and requires handling exclusively within formal access control systems.

EXHIBIT I-1

CLASSIFICATION LEVELS AND THE ASSOCIATED DEGREE OF DAMAGE

Top Secret – Unauthorized disclosure could cause ***exceptionally grave damage*** to national security.

Secret - Unauthorized disclosure could cause ***serious damage*** to national security.

Confidential - Unauthorized disclosure could cause ***damage*** to national security.

Source: Executive Order 13526

The Classification Process

When information is first identified as posing a risk to national security if disclosed without authorization, an official with "Original Classification Authority" (OCA) designates the information as classified.[10] This initial designation is referred to as the "original classification decision." The original classification decision must include a justification for why the information needs to be classified based on eight categories prescribed in EO 13526, the potential damage to national security, and the date the

[10] According to EO 13526, original classification authority is delegated by the President and the Vice President and can be further delegated by an agency head or certain other officials designated with original classification authority.

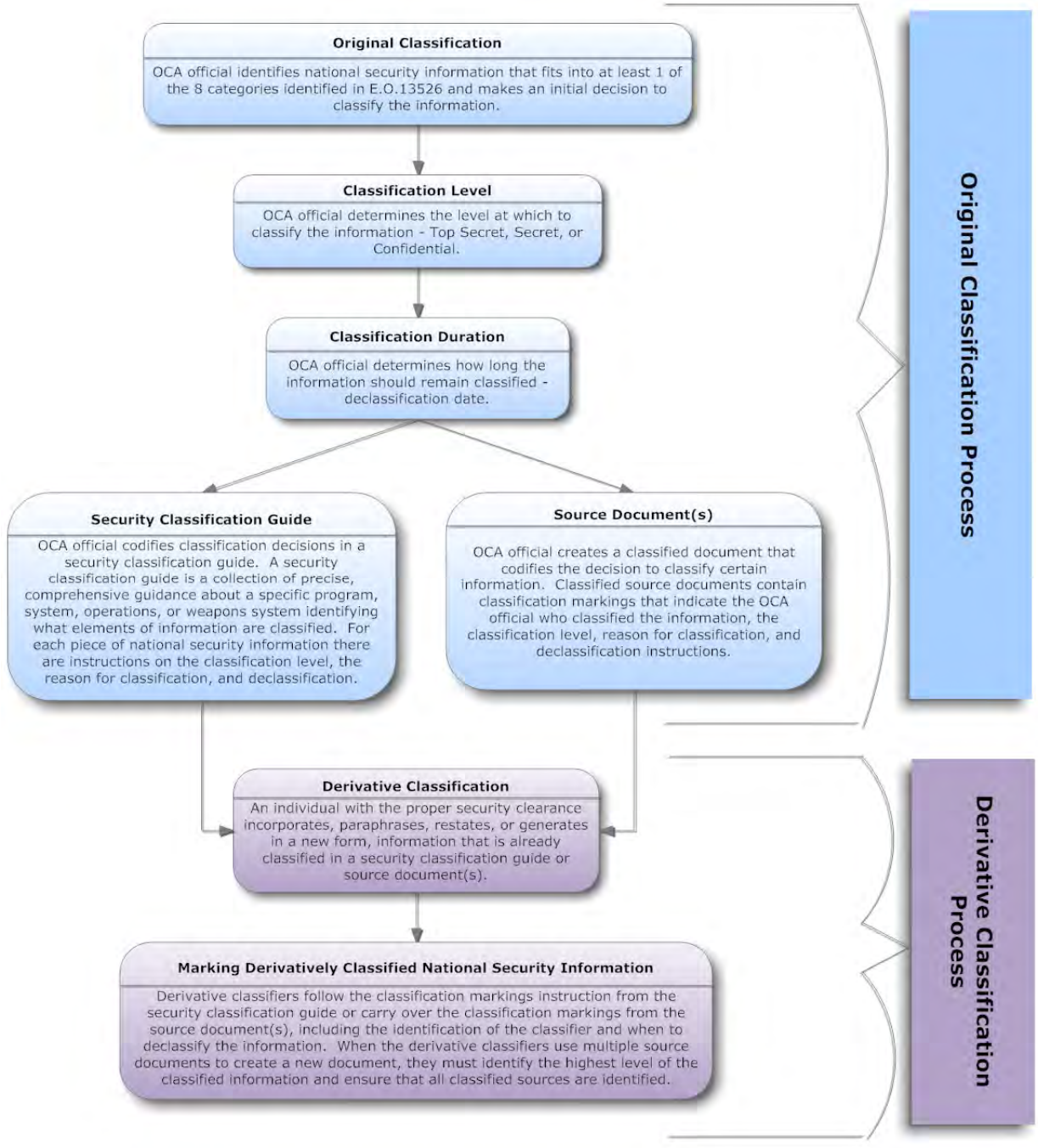
information shall be declassified.[11] OCA officials convey their original classification decisions either by marking the original document, or, more often, by including their decision in a "security classification guide" that can be used to assist in future decisions about whether to classify information in other documents.

Once an OCA official classifies specific information or issues a security classification guide identifying information categories and the appropriate classification levels, the information may be used by others in a derivative form, such as through paraphrasing, direct quotation, or summarization. When classified information is used in this manner by others after the initial designation, it also requires classification, and the information receives what is referred to as a "derivative classification decision." When making a derivative classification decision, the derivative classifier must observe and respect the original classification decision and carry forward to any newly created document the pertinent classification markings from the source document or the security classification guide.

Derivative classifiers are responsible for ensuring that the information in the documents they produce is appropriately classified and properly marked. Any individual with a current security clearance has the authority to make derivative classification decisions in conjunction with their performance of their official duties. Exhibit I-2 provides an overview of the classification process.

[11] Section 1.4 of EO 13526 prescribes the following eight categories for classified national security information: (a) military plans, weapons systems, or operations; (b) foreign government information; (c) intelligence activities (including covert action), intelligence sources or methods, or cryptology; (d) foreign relations or foreign activities of the U.S., including confidential sources; (e) scientific, technological, or economic matters relating to the national security; (f) U.S. government programs for safeguarding nuclear materials or facilities; (g) vulnerabilities or capabilities of systems, installations, infrastructures, projects, plans, or protection services relating to the national security; and (h) the development, production, or use of weapons of mass destruction.

EXHIBIT I-2
OVERVIEW OF THE CLASSIFICATION PROCESS



Source: Office of the Inspector General (OIG) Analysis of DOJ Documentation

Classification Marking Requirements

A critical part of any uniform classification management program is to ensure that standard markings or other indicia be applied to classified

information to identify the level of classification. In addition, federal agencies have a system of restrictive caveats and associated dissemination control and handling markings that can be added to a document. These markings, which are defined in classification marking guides, provide instruction on how to control and handle the dissemination of classified information. For instance, control markings might indicate that information may not be disseminated to a non-U.S. person and should include the marking, Not Releasable to Foreign Nationals (NOFORN).

To help standardize the marking of classified information throughout the U.S. government, NARA's Information Security Oversight Office has issued classification guidance and a booklet containing instructions for marking classified national security information. The NARA Information Security Oversight Office's *Marking Classified National Security Information* booklet is the baseline marking system that federal agencies are required to use to mark classified information. The booklet briefly describes how classified documents should be marked, although it also acknowledges that its guidance cannot anticipate every conceivable situation.

To supplement the Information Security Oversight Office's *Marking Classified National Security Information* booklet, ODNI established the *Intelligence Community Authorized Classification and Control Marking Manual* (Manual) through its Controlled Access Program Coordination Office (CAPCO). The CAPCO Manual, which is longer and more detailed than the Information Security Oversight Office's *Marking Classified National Security Information* booklet, prescribes a standard set of markings to be applied to classified documents and information created within the Intelligence Community, including agency-specific markings. In addition to classification markings, the CAPCO Manual includes instructions for the Intelligence Community on using markings to communicate the nature of the information, as well as dissemination control markings that indicate how and with whom the information should be shared. Unlike the Information Security Oversight Office's *Marking Classified National Security Information* booklet, which applies to all federal agencies, the CAPCO Manual only applies to members of the Intelligence Community and agencies that have an established written agreement with the Intelligence Community. Inside of DOJ, the CAPCO Manual only applies to those sections of DEA and FBI that are recognized members of the Intelligence Community.

Original and derivative classifiers are required to refer to these classification marking guides to ensure that national security information is appropriately marked, which in turn helps ensure the proper dissemination and protection of classified information. The following exhibit identifies the primary classification and control markings that should be identified on all

classified documents.[12] These classification marking requirements are for all classified information whether it is in a hard copy document, an e-mail, or another electronic form.

[12] Appendix II provides a sample document that displays these required markings.

EXHIBIT I-3

Classified Document Marking Requirements

Marking Requirement	Original Classification	Derivative Classification
Overall Classification Marking	The overall classification level must be included in a banner at the top and bottom of every classified document and indicate the highest level of classification within any portion of the document.	
Classification Block	Classified By: Identifies the Original Classification Authority by name and position or personal identifier, and the agency and office of origin. Reason: Identifies at least one of eight categories of classified information from EO 13526 1.4(a-h) Declassify On: Lists date or event by which classified information can be declassified.	Classified By: Identifies the derivative classifier by name and position or by personal identifier and the derivative classifier's agency and office. Derived From: Lists the source document(s) or the security classification guide relied upon for the classification, and the agency or office and date of the source or guide. Declassify On: Must carry forward the declassification instruction from the source document(s) or classification guide.
Portion Markings[13]	All portions of the document must be separately and properly marked with the classification of that portion. The portion marking precedes the portion to which it applies.	All portions of the document must be separately and properly marked with the classification carried over from the source document(s) or security classification guide(s) to the derivatively classified document. The portion marking precedes the portion to which it applies.
Additional Markings		
Dissemination Control Markings *(if necessary)*	Dissemination control markings are used to indicate restrictions on who may have access to the information. If dissemination control markings are necessary, they must be included in the overall marking of the document and within each portion to which they apply. The Intelligence Community requires its member agencies to include dissemination control markings on all pieces of information.	

Source: OIG Analysis of DOJ Documentation

[13] Portions may include sections, parts, paragraphs, sub-paragraphs, subjects, titles, graphics, tables, and bullets within a document.

DOJ's Classification Structure

Federal government organizations that create or hold classified information are responsible for its proper management. Classification management includes various activities, such as developing classification guides, conducting comprehensive mandatory training for classifiers, and implementing a robust self-inspection program. Within DOJ, the Director of the Security and Emergency Planning Staff (SEPS) in DOJ's Justice Management Division is the designated Department Security Officer. SEPS is responsible for implementing DOJ's classification management program and ensuring DOJ's organizational compliance with classification requirements pursuant to national security information laws, regulations, directives, and other guidance from NARA's Information Security Oversight Office and ODNI, as appropriate. SEPS established the Security Program Operating Manual (SPOM), which prescribes uniform security policies and operating procedures for the protection of classified national security information within DOJ.

SEPS relies on a Security Programs Manager in each DOJ component to implement and manage security policies and procedures within the component, including policies and procedures relating to the classification and security of national security information. Security Programs Managers are accountable to the Department Security Officer for matters related to the management and coordination of all security programs and plans within their respective organizations. In general, Security Programs Managers are responsible for administering education and training programs, overseeing physical and classification security procedures, supervising annual self-inspections, initiating risk assessments, coordinating security clearances for personnel, and reporting and resolving security violations for their respective agencies. The Security Programs Managers are the security experts for DOJ components and serve as the first line of reference for personnel who have questions related to the classification and security of national security information.

Prior Audits and Reviews

In 2004 and 2006, NARA's Information Security Oversight Office conducted on-site inspections of DOJ classification and security practices and found that improvements were needed in program management and organization, security education and training, classification guidance, tracking security violations, self-inspections, and the marking of classified documents. NARA's Information Security Oversight Office determined that DOJ needed to take corrective action to improve essential classification and security policies and procedures, including increasing resources to oversee

DOJ's classified national security information program. In addition, NARA's Information Security Oversight Office conducted reviews of the DEA and FBI classification programs in 2006 and 2009, respectively. These reviews identified classified document discrepancies, including over-classified information, missing or improper portion markings, improper use of original classification authority, incorrect declassification instructions, and information not properly referenced to source documents.

In 2006, the Government Accountability Office (GAO) also reviewed DOJ's management of classified information.[14] This review included an assessment of DOJ's implementation of NARA's Information Security Oversight Office on-site inspection recommendations. GAO reported that DOJ did not know the optimum number of staff it needed for its classification program because it had not assessed its needs and did not have a strategy to identify how it would use additional resources to address classification program deficiencies. GAO found that, as a result of these resource issues, DOJ had not fully implemented various recommendations from NARA's Information Security Oversight Office and DOJ's ability to oversee classification practices across components was insufficient.

The Office of the Inspector General (OIG) reviewed personnel security processes throughout DOJ and issued reports in September 2012 and March 2013 that included recommendations to increase resources devoted to certain security program issues.[15] These reports found that SEPS did not implement adequate personnel security processes to identify security violations and enforce security policies. Moreover, SEPS issued minimal guidance for components to follow in managing their contractor security programs and the guidance does not provide standards for maintaining accurate rosters on contract employees or periodic reinvestigations. The OIG made a total of 17 recommendations in these 2 reports to improve DOJ's timeliness in processing background investigations and adjudications, ensure that only individuals with the appropriate clearance level have access to sensitive and classified information, and improve DOJ's management of its personnel security process for contractors. These recommendations included increasing the amount of SEPS staff dedicated to conducting

[14] U.S. Government Accountability Office, *Managing Sensitive Information: DOJ Needs a More Complete Staffing Strategy for Managing Classified Information and a Set of Internal Controls for Other Sensitive Information.* GAO-07-83 (October 2006).

[15] U.S. Department of Justice, Office of the Inspector General (OIG), *Department's and Component's Personnel Security Processes.* I-2012-003 (September 2012) and OIG, *Review of the Department's Contractor Personnel Security Process.* I-2013-003 (March 2013).

security compliance reviews. Although SEPS concurred with this recommendation, at the time of the report SEPS was uncertain when it would be able allocate additional resources to compliance review efforts due to the fiscally conservative environment and the current DOJ hiring freeze.

OIG Audit Approach

Pursuant to Section 6(b) of the *Reducing Over-Classification Act*, the Inspector General of any Department with an official with original classification authority, which includes DOJ, must conduct two evaluations to: (1) assess whether applicable classification policies, procedures, rules, and regulations have been adopted, followed, and are effectively administered within such department, agency, or component; and (2) identify policies, procedures, rules, regulations, or management practices that may be contributing to persistent misclassification of material within such department, agency, or component. The *Reducing Over-Classification Act* requires the first evaluation to be completed by September 30, 2013, which this audit report satisfies. The second evaluation, which is due by September 30, 2016, will review DOJ's progress implementing the recommendations of this audit.

Section 6(b) of the *Reducing Over-Classification Act* also requires individual Inspectors General coordinate to ensure that the evaluations follow a consistent methodology. In accordance with this requirement, the ODNI Office of the Inspector General and the Department of Defense Office of the Inspector General established an Inspectors General Working Group to develop a standardized approach for the first evaluation. We participated in the Inspectors General Working Group and used the standardized evaluation guide during the course of our review. However, the DOJ OIG's audit focused exclusively within DOJ, and we have not conducted any cross-agency comparisons of classification policies and practices. We are therefore unable to assess whether different agencies treat the same information the same way.

During this audit, we conducted over 100 interviews with officials from SEPS, the FBI, the DEA, the Criminal Division, the National Security Division, and the United States Marshals Service (USMS).[16] In addition, we reviewed 10 security classification guides and a sample of 141 classified documents created during fiscal year (FY) 2012 comprised of finished reports, memoranda, legal documents, summary reports, e-mails, case file documents, Intelligence Information Reports (IIR), and DEA Analysis

[16] For more information about our audit scope and methodology, see Appendix I.

Reports. During our review, we also reviewed classified information from programs that require special access controls.[17]

The results of our review are detailed in Findings I and II. Finding I provides the results of the OIG's evaluation of DOJ's classification policies, processes, and practices, including a review of DOJ's classified national security information decisions and its use of classification management tools. Finding II provides our analysis of DOJ's management and oversight of the classification program, including an overview of DOJ's implementation of statutory and regulatory requirements.

[17] Due to the sensitivity of the classified information related to these programs, the responsible component instituted special access controls, including logging the individuals who are granted access, providing these individuals a "read-on briefing" to present background information on the program, and requiring the individuals to sign a non-disclosure agreement.

FINDINGS AND RECOMMENDATIONS

I. DOJ CLASSIFICATION POLICIES, PROCESSES, AND PRACTICES

DOJ has established classification policies and procedures, but has not effectively administered those policies and procedures to ensure that information is classified and disseminated appropriately. Although our review of a small sample of documents did not find indications of widespread misclassification, we did identify deficiencies with the implementation of DOJ's classification program, including persistent misunderstanding and lack of knowledge of certain classification processes by officials within various DOJ components. We also found various classification marking errors throughout the classified documents we reviewed. These marking errors stemmed from reliance on historical practices and had been overlooked because of inadequate training and oversight. We believe that DOJ could improve its classification program by enhancing security classification and marking guides to better explain why and how information is classified, and by using existing automated tools to improve classification and marking practices. Moreover, we believe that SEPS should work with component Security Programs Managers to improve personnel training on classification requirements, procedures, and guidance.

DOJ Original and Derivative Classifiers

The act of original classification requires that an OCA official identify the elements of information regarding a specific subject that must be classified, describe the damage to national security that could reasonably be expected if the information is disclosed, determine how long that information needs to be protected, and document these decisions in a security classification guide or to the original (source) document.[18] Derivative classifiers must interpret the OCA guidance from the classification guide or from various source documents and determine how to mark classified products they produce.

Pursuant to EO 13526, the President has delegated original classification authority to the Attorney General, who has further delegated

[18] An element of information is a specific piece of information related to an overall subject area that an OCA official has determined meet the requirements for classification.

original classification authority to 63 DOJ officials from 13 components. In addition, DOJ has nearly 60,000 personnel that hold security clearances and are therefore eligible to derivatively classify information in the performance of their duties. Exhibit 1-1 identifies the number of DOJ personnel by component with authority to make original classification decisions, as well as those who can derivatively classify information.

EXHIBIT 1-1

DOJ Officials with Original and Derivative Classification Authority as of April 2013

DOJ Component	OCA Officials	Derivative Classifiers
Office of the Attorney General	2	17
Office of the Deputy Attorney General	3	45
Office of the Associate Attorney General	1	8
Office of the Inspector General	1	421
Antitrust Division	1	79
Bureau of Alcohol, Tobacco, Firearms, and Explosives	1	4,224
Criminal Division	7	749
Drug Enforcement Administration	20	7,160
Federal Bureau of Investigation	17	35,951
Federal Bureau of Prisons	1	14
Justice Management Division	2	524
National Security Division	7	364
U.S. Marshals Service	1	3,096
All Other DOJ Components[19]	0	5,327
TOTAL	**64**	**57,979[20]**

Source: SEPS

According to EO 13526, the delegations of OCA officials shall be limited to the minimum required to ensure the consistency and integrity of classified national security information, and agency heads are responsible for ensuring that designated subordinate officials have a demonstrable and continuing need to exercise this authority. To ensure that DOJ had the appropriate

[19] According to the list provided by SEPS, there were 28 DOJ components that comprised the "all other DOJ components" category as of April 2013.

[20] These figures were obtained from SEPS and represent the number of people in its database of security clearance holders. This figure only includes full-time DOJ employees and does not include DOJ contractors who have security clearances and are able to derivatively classify information. We did not verify these figures with each component and they were not used in the development of our conclusions or recommendations.

number of OCA officials, DOJ conducted a Department-wide evaluation between fiscal years (FY) 2011 and 2012. SEPS directed each component to determine which positions require original classification authority and to reduce the number, if possible. SEPS concluded its review in July 2012 and proposed to reduce the number of DOJ OCA officials by 38, from 102 to 64. The Attorney General approved these changes in April 2013.

The OIG found that DOJ's reduction of OCA officials was the result of the FBI reducing its number of OCA officials from 55 in FY 2012 to 17 in FY 2013. During this initiative, the Criminal Division, the National Security Division, and the DEA did not reduce the number of authorized OCA officials. Although the DEA previously reduced its number of positions with original classification authority in 2007, the DEA maintained its level of 20 OCA officials from FY 2012 to FY 2013 even though only 7 of these 20 OCA officials made "original classification decisions" in FY 2012. In addition, although the National Security Division did not reduce the number of OCA officials during the SEPS review, National Security Division officials informed the OIG that the number of OCA officials could be decreased by at least one.

Based on our review of types of information classified within DOJ, we believe that the frequency in which information is classified in the first instance should be extremely rare. Therefore, having more individuals with original classification could contribute to information being classified at different levels and retained for varying periods of time. As a result, we believe that the number of OCA officials within DOJ could be further reduced, particularly at the DEA, which has the highest ratio of DCA officials to OCA officials at 358 to 1, as illustrated in Exhibit 1-1. In comparison, the FBI, the largest component within DOJ, has a DCA-to-OCA ratio of 2,115 to 1, and the DOJ-wide ratio is 905 to 1. We recommend that SEPS, in conjunction with the components, re-evaluate the number and types of positions that require original classification authority to ensure compliance with EO 13526.

DOJ Security Classification Guides

Security classification guides contain original classification decisions and provide derivative classifiers with a set of instructions from an OCA official to use when making derivative classification decisions. Security classification guides identify predetermined classification decisions on various topics of program-specific information, the classification level of that information, the nature of the risk to national security, the length of time the information should remain classified, and the reason for classification, which identifies the specific category of national security information from Section 1.4 of EO 13526 into which the information falls. As an example,

Exhibit 1-2 includes an excerpt from the *DOJ's National Security Information Security Classification Guide*.

EXHIBIT 1-2

Example of a DOJ Security Classification Guide Element

Item No.	Category of Information	Classification Level	Declassify On	Classification Reason[21]
2	Individually unclassified or controlled unclassified data items that the compilation would provide insight into DOJ's functions, staffing, activities, capabilities, vulnerabilities, or intelligence sources and methods.	Confidential	+25 years	1.4 (c), (g)

Source: *DOJ National Security Information Security Classification Guide*

In FY 2012, DOJ had ten approved security classification guides: one comprehensive guide established by SEPS for Department-wide use and nine additional guides created by the FBI, DEA, Criminal Division, and USMS for use by the individual components. The SPOM requires DOJ components to submit initial and updated security classification guides to the Department Security Officer for approval. The following exhibit provides the number of SEPS-approved DOJ security classification guides by component as of July 2013.

EXHIBIT 1-3

Approved DOJ Security Classification Guides as of June 2013

DOJ Component	Approved Security Classification Guides
SEPS/Department-wide	1
Criminal Division	1
DEA	1
FBI	6
USMS	1
Total	**10**

Source: SEPS

[21] See footnote 11 for the eight approved classification categories that correspond to classification reason codes.

In general, we found that all security classification guides in use throughout DOJ met the minimum requirements established by SEPS, including, but not limited to, identifying the types and specific topics of information deemed classified and identifying reasons for classifying the information, the level at which the information should be classified, and the duration of the classification. However, we also found that DOJ had not sufficiently coordinated the creation of security classification guides and that some of the security classification guides used throughout DOJ could benefit from additional clarification on specific details to optimally ensure that derivative classifiers of DOJ information could make informed and accurate classification decisions. These issues are discussed further below.

Creation of Security Classification Guides

In 2008, ODNI issued a report on classification guidance stating that a critical component of effective intelligence collaboration and information sharing is a common understanding of information classification standards and policies.[22] The report further noted that inconsistent interpretation and application of the classification levels defined by agencies can result in uneven guidance, misunderstanding, and a lack of trust between Intelligence Community agencies and mission partners concerning the proper handling and protection of information. Moreover, the report cited variations and conflicts among classification guidance as having the potential to slow or prevent critical information sharing among agencies, governments, and other national security partners.

During our review, we found that the creation of security classification guides was not well coordinated by SEPS, component Security Programs Managers, and other officials responsible for overseeing component-level programs that routinely handle mission-specific national security information. SEPS established the *DOJ National Security Information Security Classification Guide*, which was intended for Department-wide use. In developing the guide, SEPS relied upon component Security Programs Managers to consult others within their components to ensure the guide appropriately accounted for the types of information that would be encountered by derivative classifiers using the guide. However, we found that some component Security Programs Managers did not confer with pertinent offices during the review and acceptance of the content. Further, some DOJ components created additional security classification guides for

[22] ODNI, *Intelligence Community Classification Guidance Findings and Recommendations Report*, January 2008.

their programmatic use without fully coordinating with SEPS or, in at least one instance, with other affected components.

Specifically, the *DOJ National Security Information Security Classification Guide* includes guidance related to Foreign Intelligence Surveillance Act (FISA) processes. Yet according to some National Security Division officials interviewed, the National Security Division, which performs various FISA-related activities, was not involved in the development of this guidance, and as of May 2013, National Security Division officials, including attorneys who work with FISA-related information, were unaware that this guidance existed. During interviews with the OIG, SEPS and National Security Division officials acknowledged this discrepancy and agreed that the National Security Division should work with SEPS to incorporate into the *DOJ National Security Information Security Classification Guide* all relevant requirements, policy decisions, and processes related to classified national security information in the National Security Division or specifically related to FISA processes. In addition, the National Security Division has taken steps to improve its employees' awareness of the *DOJ National Security Information Classification Guide* by including a link to the guide on National Security Division intranet site.

We also found that the USMS established a security classification guide in FY 2012, the *USMS Operations and Capabilities Security Classification Guide*, that contains many of the same national security information already identified in the *DOJ National Security Information Security Classification Guide*. As a result, SEPS officials told us that, in their opinion, it was unnecessary for the USMS to have its own security classification guide. According to USMS officials in charge of producing the USMS guide, SEPS did not inform them and they did not inquire about the possibility of incorporating national security information specific to the USMS into the *DOJ National Security Information Security Classification Guide*. Nevertheless, USMS officials agreed that its guide could be integrated into the *DOJ National Security Information Security Classification Guide*. Following our inquiries, SEPS informed us that as of July 2013 the USMS's security classification guide was not being utilized nor was it approved for use within the USMS. In August 2013, SEPS and the USMS began coordinating to integrate the USMS's needs into the DOJ-wide guide and ensure that the *DOJ National Security Information Security Classification Guide* is utilized effectively within the USMS.

In addition, we found that the Criminal Division created a security classification guide in July 2012 for classifying and handling information for a joint program the Criminal Division administers with the DEA, but that despite sharing original classification authority over the relevant information

with DEA officials, the Criminal Division did not actively involve the DEA when creating the guide. As a result, the DEA declined to use the Criminal Division's security classification guide because it did not adequately address all of DEA's needs and issues. Moreover, one DEA official told us that the DEA would probably develop its own, parallel classification guide for the program.

According to SEPS officials, when the Criminal Division first created the security classification guide, officials were instructed to ensure that all participants in the program were included in making the classification decisions and establishing instructions for classifying national security information within the guide. Nevertheless, SEPS approved the security classification guide without verifying with the DEA that all necessary requirements and instances of national security information were incorporated.

At the audit close-out meeting, SEPS officials reiterated to the OIG that they relied upon DOJ components' Security Programs Managers to coordinate with all OCA officials, subject matter experts, and any other agency affected by the creation of security classification guides. Moreover, SEPS officials stated that SEPS's approval of DOJ component's security classification guides is basically an "administrative action" because SEPS does not have the subject matter expertise with regard to specific program classification requirements. SEPS only reviews the security classification guides for basic form and function. Therefore, SEPS officials believe that DOJ component's OCA officials and Security Programs Managers should be accountable for the content of the information in program-specific DOJ security classification guides.

We agree with SEPS's assessment that DOJ components' Security Programs Managers should be held accountable for consulting with all interested parties to ensure that the content of security classification guides is accurate and useful for all purposes. However, we attribute the lack of coordination on security classification guides to a general unfamiliarity in DOJ with the purpose and importance of security classification guides. We also believe that SEPS has a responsibility to ensure that the Security Programs Managers and OCA officials understand the importance of consistent, comprehensive, and accurate security classification guides.

As recognized by ODNI in its 2008 report, we believe that fewer security classification guides would help ensure consistency of classification decisions across DOJ, as the development of separate security classification guides regarding the same classified information can lead to different, and potentially conflicting, marking and handling requirements for the same

classified information, thereby increasing the risk of marking and handling errors and complicates users' efforts to comply with the guides. We therefore recommend that SEPS should ensure that DOJ components are aware of and understand how to use security classification guides. Moreover, to increase efficiency and classification accuracy, we recommend that SEPS review all DOJ security classification guides and work with DOJ component Security Programs Managers and OCA officials to identify and reduce redundancies.

Security Classification Guide Assessment

During our review of DOJ's ten security classification guides, we found that some of these guides did not provide adequate instruction on when and at what level to classify information. For instance, as shown in Exhibit 1-2 the *DOJ National Security Information Security Classification Guide* instructs users to classify as confidential the following: "individually unclassified or controlled unclassified data items that the compilation would provide insight into DOJ's functions, staffing, activities, capabilities, vulnerabilities, or intelligence sources and methods." However, the security classification guide does not explain what types of unclassified or controlled unclassified data items, if combined, would result in classification. We also found that some of the security classification guides identified national security information and then instructed the classifier that the classification of this information could range from unclassified to Top Secret without fully explaining the circumstances that would cause the level of classification of the information to escalate from one level to another. Insufficient, ambiguous, and over-broad explanations such as these provide inadequate guidance to derivative classifiers and could result in the misclassification of information.

We also found that the *DEA National Security Information Security Classification Guide* contained inconsistent internal elements that identify different ways to classify the same information. For instance, the *DEA National Security Information Security Classification Guide* identifies two elements associated with foreign government information provided in confidence and identifies in one element that the information should be identified as unclassified law enforcement sensitive information, while the other element instructs users that the information should be classified as Secret. No guidance is offered about the different circumstances that would cause a derivative classifier to apply one instruction as opposed to the other. We believe that these ambiguous and seemingly contradictory instructions are likely to result in a derivative classifier marking Secret information as "Unclassified, law enforcement sensitive," or marking unclassified information as Secret.

We found that the FBI's security classification guides often provided the best explanations regarding the circumstances that would require the specific classification of information. For example, the *FBI National Security Information Classification Guide* contains almost two pages and three separate line items devoted to the appropriate classification of case numbers and other case-specific identifying information. This section of the FBI guide contains explicit instructions and examples for FBI employees, such as:

- "The fact that a numeric and alpha designation, such as 134A or 315H, is or could be an FBI case file number." The FBI guide then provides two specific examples, including: "An agent calls his supervisor and tells him/her 'I'm working a 415J matter' would be unclassified."

- "Association of case file number with specific threat countries and/or organizations in a national security program" is to be classified Secret and the guide goes on to provide four additional instructions (similar to the bullet above) and an explanation why the information is sensitive and needs to protected.

By contrast, the *DOJ National Security Information Security Classification Guide* states that information providing "specific details of relationships between DOJ and members of the Intelligence Community" should be classified at the Secret level. However, the DOJ guide does not provide a definition or examples of the "specific details" that warrant classification or the potential damage if the information were released. We believe that specific instructions for derivative classifiers, similar to those provided in the FBI guide, are likely to reduce instances of misclassification and mishandling of national security information.

According to SEPS officials, DOJ personnel who use a security classification guide should have a basic understanding of what type of information must be classified and also have a responsibility to contact their Security Programs Managers to request clarification and additional guidance when needed. Nevertheless, DOJ officials who are considered classification subject matter experts told us that DOJ should clarify and refine instructions in its security classification guides to reduce the likelihood of confusion and misunderstanding among derivative classifiers. We agree, and we recommend that SEPS review all DOJ security classification guides to ensure that instructions are clear, precise, consistent, and provide derivative classifiers with sufficient information to make accurate classification decisions.

DOJ's FY 2012 Classification Decisions

In FY 2012, DOJ components with OCA officials reported a total of 4,689 original classification decisions and over 8 million derivative classification decisions, as shown in Exhibit 1-4.[23]

EXHIBIT 1-4

FY 2012 Classification Decisions[24]

DOJ Component	Original Classification Decisions	Derivative Classification Decisions
Bureau of Alcohol, Tobacco, Firearms, and Explosives	0	105
Criminal Division	603	231
Drug Enforcement Administration	849	80,953
Federal Bureau of Investigation	4	8,355,880
Justice Management Division	0	54
National Security Division	3,232	280
Office of the Inspector General[25]	0	185
U.S. Marshals Service	1	0
Total	**4,689**	**8,437,688**

Source: SEPS

We reviewed a judgmental sample of 25 original classification decisions from the National Security Division, Criminal Division, and DEA and 116 derivative classification decisions from the National Security Division, Criminal Division, FBI, and DEA.[26] Our review identified several discrepancies, including incorrect designations of decisions as "original"

[23] Classification decisions include all actions in which an OCA official initially determines that information should be classified and each time derivative classifiers incorporate, paraphrase, restate, or generate in a new form, information that is already classified.

[24] This chart only reflects DOJ components with at least one OCA official that made at least one original or derivative classification decision during FY 2012.

[25] Although the OIG reported derivative classification decisions during our audit period, we excluded the OIG from our review to avoid a conflict of interest.

[26] The OIG judgmentally selected a sample of classified documents with the intent of obtaining broad exposure to the classified work performed within DOJ components during FY 2012 and we focused our review on the four components with substantial numbers of classification activity during FY 2012. The FBI only made four original classification decisions in FY 2012 and all four of these decisions were the creation of security classification guides. Because we assessed the adequacy of security classification guides separately, we did not include these documents in our testing of original classification decisions. A more detailed description of our sample selection methodology for each component is in Appendix I.

classification decisions, information that had been inappropriately identified as classified (over-classification), improper use of a dissemination control, and unmarked or incorrectly marked documents containing classified national security information.

Original Classification Designations

We found that the National Security Division, Criminal Division, and the DEA incorrectly designated classified information as "original" classification decisions. The documents we reviewed that were identified as containing original classification decisions in fact contained information that previously had been identified as classified in at least one source document or in a security classification guide. Therefore, these decisions should have been identified as derivative classification decisions, not original classification decisions. Based on interviews with component officials, we found that each of these DOJ components had a different process and reason for designating the classification as original decisions instead of derivative decisions.

National Security Division – Among its other responsibilities, the National Security Division processes applications for FISA warrants. During our review, we found that the National Security Division categorized the classification of all FISA applications and all FISA-related documents as original classification decisions. Yet we found that the National Security Division was creating these documents, in part, using classified national security information submitted by other government agencies. Moreover, according to National Security Division officials, all applications for FISA authorities are classified at least at the Secret level.[27] National Security Division officials explained that historically DOJ has applied original classification decisions to applications and other FISA-related pleadings before the Foreign Intelligence Surveillance Court (FISA Court). National Security Division officials believe that this practice emerged because even though much of the information in the FISA documents are supplied by the Intelligence Community, DOJ represents the United States before the FISA Court and is responsible for the form of the information provided in FISA applications and related documents. This policy determination, which established a National Security Division-wide protocol for classifying FISA-specific information, represented an original classification decision, and the subsequent classification of any information meeting the criteria of this decision is therefore a derivative classification decision. Consequently, the

[27] This classification meets the requirements of Section 1.4 of EO 13526, which includes intelligence sources or methods as a category of information that shall be classified.

National Security Division erred by categorizing the documents we reviewed as original classification decisions.

National Security Division officials, including an OCA official, agreed that the National Security Division's FISA-related information that had been identified as original classification decisions could more accurately be identified as derivative classification decisions. However, some of the National Security Division officials were unfamiliar with the derivative classification process, despite generally following derivative classification procedures by carrying over classification markings from source documents. National Security Division officials also told us they were apprehensive about fully implementing the derivative classification process because they believed it would slow down the National Security Division's processes related to its FISA work. Nevertheless, the National Security Division's Director for Security stated that the National Security Division would begin to implement derivative classification procedures and agreed that they would work with SEPS to update the Department's classification guide to help implement such a change. We expect that when the National Security Division implements this change in procedure, its reported number of original classification decisions, as illustrated in Exhibit 1-4, will decrease significantly.

Criminal Division – The Criminal Division develops, enforces, and supervises the application of federal criminal laws in coordination with other government agencies, including DOJ components. We reviewed Criminal Division documents containing classification decisions categorized as original decisions by an OCA official and found that all of these documents did not meet the criteria for an original classification decision because the classified information in each of the documents had been incorporated previously into a security classification guide created specifically for the Criminal Division's limited-access classified program.

When the OIG asked this official why he had not derivatively classified the information using the security classification guide that he created, the OCA official stated that he was unsure of the difference between original and derivative classification decisions, and that he believed that by classifying the document as an original decision he could better control who received the information and how the information was used. However, this practice obviates the benefits of a classification guide and creates the potential for setting inconsistent declassification dates.

Although this OCA official had received classification training and worked directly with SEPS on the creation of the security classification guide, the official continued to use improper classification processes. After our

identification of the issue, Criminal Division and SEPS officials met and agreed that it was appropriate to classify the information derivatively using the security classification guide. We believe that when the Criminal Division implements this change in practice, its reported number of original classification decisions, as illustrated in Exhibit 1-4, will decrease significantly.

Drug Enforcement Administration – As part of its mission, DEA is responsible for enforcing the controlled substances laws and regulations of the United States, as well as recommending and supporting non-enforcement programs aimed at reducing the availability of illicit controlled substances domestically and internationally. We found that the DEA was improperly classifying documents using original classification authority when the information in these documents previously had been classified in a security classification guide. A DEA official stated that he believed information was better protected from widespread dissemination when the classifier used original classification decisions rather than derivative classification decisions. However, this OCA official also acknowledged that the DEA's information did not fit the criteria for an "original" classification decision, although he expressed uncertainty when asked whether the DEA would revise its processes for classifying the information.

In its 2006 review of the DEA, NARA's Information Security Oversight Office identified this same discrepancy. NARA's Information Security Oversight Office briefed the DEA on the proper process for classifying previously identified classified information and informed the DEA that it should include the information in a security classification guide. The DEA responded to the NARA review on May 8, 2007. In its response, the DEA acknowledged that it was incorrectly making original classification decisions and informed NARA's Information Security Oversight Office that the DEA's two major producers of classified documents were engaged in producing local classification guides that would be used to supplement a DEA classification guide that was in draft at the time. The DEA anticipated that its actions would result in an increase of the number of derivative classification decisions versus the number of original classification decisions currently being made by the DEA. According to the DEA, its original classification decisions were reduced by 85 percent in FY 2012 as compared to the previous 3 years. However, despite the DEA's efforts, our review found that the DEA continues to improperly use original classification decisions, as explained above.

We believe the DEA should revise its classification processes and practices to comply with DOJ security and classification procedure

requirements. We also believe that, if the DEA corrects its process for classifying information, its reported number of reported original classification decisions, as reflected in Exhibit 1-4, will decrease significantly.

Originally classifying information that was previously classified can inadvertently alter the dissemination controls or extend the declassification period. For instance, if an OCA official takes information from a source document that has a declassification date set for 25 years from 2002 and creates a new document that is categorized as an original classification decision, the OCA official can extend the declassification date to 25 years from the date the new document was created, resulting in inconsistent declassification dates for the same information. Moreover, because originally classified documents do not identify any source materials, there is no way to trace the information in the new, originally classified document back to the previously classified document to ensure that all markings are identical, raising the possibility of inconsistent handling instructions for the same information. Incorrectly applying OCA classification markings can also increase the risk that the same information would be classified differently across programs because different OCA officials could, in theory, reach different conclusions about the appropriate classification of the same information. Additionally, improper classification processes increase the likelihood that classified information will be mishandled, and as a result can undermine the trust and confidence that is necessary for critical sharing of national security information among and within federal agencies.

Based on our findings, we believe that SEPS and DOJ component Security Programs Managers have not emphasized to OCA officials the importance of the standardized classification process. SEPS should work with DOJ component Security Programs Managers to ensure that OCA officials understand the difference between original and derivative classification decisions and properly mark classified information according to the proper requirements of the classification decisions.

Review of Classification Levels

Although we did not find widespread misclassification during our limited review of classified DOJ documents, we found several documents in

which information was inappropriately identified as being classified.[28] We discussed the specifics of these findings with the components. The following are some examples of over-classified information found by the OIG and the response from officials at various DOJ components.

At the National Security Division, we identified one report (erroneously classified as an original decision) as over-classified because the information did not meet one of the eight reasons for classification. The report referred to FBI classified material, but did not provide specific information about FBI classified programs or cases that would justify its classification. National Security Division officials stated that their practice was to follow FBI practices regarding classification, and because the FBI classifies certain national security programs and cases, they decided to classify the report. Moreover, a National Security Division official explained that they are sensitive to the aggregation of information that could be manipulated to expose sensitive program details. However, these officials understood the OIG's assessment that, because the information contained in the report did not provide classified details, the information should not have been classified and agreed to review the classification of future reports.

At the FBI, we identified a terrorist watchlist nomination document that was classified by the preparer. Because the terrorist watchlist is an unclassified subset of terrorism information, the OIG asked the FBI official responsible for the document why the information in the document was classified. The official explained that he was unaware of the FBI's classification requirement for watchlist nominations and was following previous work experience practices from another Intelligence Community agency. This official agreed with the OIG that the information should have been marked unclassified.

We also found that the National Security Division and the Criminal Division over-classified portions in otherwise properly classified documents that contained standard language citing unclassified laws, statutes, or regulations. The Criminal Division official who classified the information

[28] Key terminology, such as "over-classification" and "damage to national security" has not been defined by law, regulation, or executive order. During the course of our evaluation, we used a working definition of "over-classification," which was supplied by NARA's Information Security Oversight Office: the designation of information as classified when the information does not meet one or more of the standards for classification under section 1.1 of EO 13526. For example, "over-classification" can occur when information is marked classified but does not fall into any of the eight categories of information specified by EO 13526. In addition, "over-classification" occurs when information is classified at too high of a level, such as information that might be marked Top Secret but for which unauthorized disclosure would not cause "exceptionally grave damage to national security."

agreed with the OIG's assessment that the information should not have been classified. The National Security Division official who reviewed the classified information in the OIG sample documents opined that the information was classified appropriately because the inclusion of certain language from laws, statutes, or regulations could expose the nature of the classified program. However, this official concurred with the OIG that statements of general policy that are devoid of derivation or application to specific classified operations should not be marked classified.

Persistent misunderstanding and unawareness of proper classification processes can cause misclassification, which requires additional expenditures of funds and commitments of resources to store and secure the information and reduces the transparency of government operations.[29] Although our limited review only found isolated instances of over-classified information, the types of weaknesses we identified throughout our review were associated with DOJ's implementation of information classification policies and procedures, leading us to believe that DOJ is susceptible to additional instances of misclassification.

Proper Use of Dissemination Controls

During our review of DEA classified documents, we found that the DEA added to some of its classified information the control marking, "Originator Controlled" (ORCON), with some also including additional warning caveats on the use of the information. According to the CAPCO manual, ORCON is used on classified intelligence that clearly identifies or reasonably permits ready identification of intelligence sources and methods that are particularly susceptible to countermeasures capable of nullifying or measurably reducing their effectiveness. The DEA's Office of National Security Intelligence must adhere to the CAPCO manual requirements because it is a member of the Intelligence Community. However, we found that DEA offices within and outside of the Intelligence Community both used the ORCON dissemination control and we believe that some of the information in the classified DEA documents that we reviewed did not meet the CAPCO manual's ORCON definition. According to one DOJ official, it is difficult for an agency to deal with ORCON marked documents because it inhibits sharing of information. Moreover, this official explained that individuals may also be unaware of what the ORCON marking actually entails and people may not be following the instruction for getting authorization from the source to further share the information.

[29] According to NARA's Information Security Oversight Office, the total security classification cost estimate within the government for FY 2012 was $9.77 billion.

DEA officials told us that although the DEA's preference was not to use the ORCON dissemination control and additional warning caveats, the DEA had adopted the restrictions for the protection of ongoing investigative information or confidential source information. Officials explained that the ORCON marking and warning caveats were necessary to help ensure that others receiving the information do not act on or share the information without first "deconflicting" operational activities or coordinating their information sharing efforts with the DEA. Additionally, DEA officials told us that even with the addition of the ORCON control markings, the DEA has had other government agencies misuse their information and in some cases this has resulted in the compromise of an ongoing operation or damage to relations with a foreign nation. He also stated that including the ORCON marking and warning caveat was the DEA's attempt to better protect its information by instructing recipients to consult with the DEA before any action is taken based on DEA information.

We believe that the use of the ORCON dissemination control is necessary to protect certain types of classified information. We also recognize that law enforcement components within the DOJ have a need to protect their on-going investigations and operations. From our conversations with DEA officials, it appears that the type of protection that the DEA is trying to achieve through its use of ORCON is not currently being affected by its use of the ORCON control marking. In addition, it appears that the non-Intelligence Community DEA entities using the ORCON control markings are doing so improperly. According to a SEPS official, overuse of dissemination control markings like ORCON dilute the effectiveness of these markings. Therefore, we believe that it is possible that the DEA's expanded use of the ORCON dissemination control marking is reducing its usefulness.

According to SEPS officials, the onus is on DOJ components that use the ORCON dissemination control to ensure that personnel understand the purpose of the ORCON dissemination control and use it appropriately. Moreover, SEPS officials stated that ODNI was developing ORCON-specific training and SEPS will promulgate that training once it is finalized. Because the use of the ORCON dissemination marking may also impede the timeliness for which classified information can be shared between agencies, we recommend that SEPS ensure that ODNI's ORCON-specific training is promulgated to DOJ components once it is issued. In addition, SEPS should coordinate with the DEA Security Programs Manager and officials representing all DEA entities using the ORCON control markings to ensure that the DEA's use of dissemination control markings is appropriate.

Classification Marking Deficiencies

During our review of classified documents, we found many documents that either did not contain required classification markings or contained incorrect classification markings. When we brought these issues to the attention of DOJ officials within these components, they generally agreed with the OIG's assessments. Exhibit 1-5 provides an overview of the marking errors identified by the OIG.

EXHIBIT 1-5

Classified Document Marking Errors

Sample of FY 2012 Documents Reviewed by the OIG	DOJ Components				
	FBI	**National Security Division**	**Criminal Division**	**DEA**	**Total Documents Reviewed**
Derivative Classification Decisions	56	20	16	24	**116**
Original Classification Decisions[30]	0	11	10	4	**25**
Marking Errors on Documents Reviewed[31]					**Total Marking Errors**
Classification Block Errors					
Missing, Incomplete, or Incorrect "Classified By" Information	51	20	16	0	**87**
Missing, Incomplete, or Incorrect "Derived From" Information	52	18	16	8	**94**
Missing, Incomplete, or Incorrect Declassification Instructions	5	15	17	0	**37**
Missing Portion Markings	25	9	18	9	**61**
Missing or Incorrect Dissemination Control Markings	23	5	10	8	**46**
Missing or Incorrect Classification Banner	14	7	10	1	**32**
Totals	**170**	**74**	**87**	**26**	**357**

Source: OIG Review of DOJ Documents

Within this sample, we reviewed classified meeting notes and e-mails. We found that officials often did not properly mark these documents because

[30] We reviewed the "original classified" documents for proper classification markings using the requirements for original classification decisions. However, as noted previously, these documents should have been derivative classification decisions. These documents were not evaluated to ensure that the source information was identified because original classification decisions are only required to identify the OCA official and the intent of DOJ components at the time of our audit was to make original classification decisions.

[31] The identified marking errors exceed the number of documents reviewed because in many cases, a single document contained multiple marking errors.

they were unaware of the classified marking requirements for these classified products. As an example, we reviewed a document containing the synopsis of a classified meeting over a secure phone call with a National Security Division official and officials from Intelligence Community agencies that was marked with an overall classification of Secret, but because the National Security Division official was unsure about other classification and marking requirements for meeting notes, the document did not include the required classification block or portion markings. Similarly, Criminal Division officials stated that they often discuss classified information at meetings with members of the Intelligence Community but were unsure about how to classify and mark their notes from these conversations.

We also found that although some classified DOJ component e-mails contained an overall classification marking, the majority of the e-mails that we reviewed did not contain any classified portion markings or a classification block. In addition, classified e-mails did not contain the classification banner. Officials explained that they were not aware of classification and marking requirements for forwarding a classified e-mail, and they did not understand their responsibilities when replying to an e-mail that lacked appropriate classification markings. As a result, a single marking error in an e-mail can be propagated many times over through replies and forwards.

Missing, Incomplete, or Incorrect Classification Block Information – Generally we found that the identification of the classifier was not included in the classification block. Moreover, we found that some components did not include a classification block on documents or included an original classification block on a derivatively classified document. Further, some components used out-of-date classification guidance or included outdated versions of security classification guides. When we asked why the documents contained incomplete or incorrect classification blocks, FBI, DEA, National Security Division, and Criminal Division officials stated either they were unaware of the classification block requirements or were using outdated templates, tools, or previously classified documents to provide the format or information for their classification block.

Lack of or Incomplete Source Reference – We found that none of the documents that used multiple sources to derive a classified document properly referenced the source documents in the classification block or included a classified addendum. Although the implementing regulation and DOJ policy clearly identify this requirement, FBI, DEA, National Security Division, and Criminal Division officials stated that they were unaware of the source list requirements. Criminal Division and National Security Division officials said that they generally attach the source documents to the file copy

of the document. These officials added, however, that there are instances in which the drafting attorney needs additional information and will contact the source of the information directly and could place that information in Criminal Division and National Security Division case files. However, the files reviewed by the OIG did not contain source information for all of the classified information contained in the documents.

Incorrect Declassification Instructions – FBI, National Security Division, and Criminal Division officials were also unfamiliar with requirements for declassification markings. We found that classifiers generally used "25 years from the date of creation" as the "de facto" declassification date and did not consult security classification guides for the OCA official's declassification instructions. Additionally, some of these officials were unaware of the requirements for determining a declassification date on a classified document that was created using information from multiple sources. In these circumstances, classifiers are required to use the declassification instruction that corresponds to the longest period of classification among all of the source documents, yet many of the officials we interviewed stated that they instead made an educated guess to determine the declassification date. Because these practices can result in information remaining classified longer than may be necessary, there is an increased risk of wasted resources, such as security containers and security guards needed to protect the information from disclosure. Conversely, if classifiers improperly use a period shorter than necessary, classified information may inadvertently be exposed before the risk to national security has passed.

Missing Portion Markings – In our review of a sample of classified information, we found 63 occurrences where the classifier failed to properly apply portion markings to a document with the appropriate classification level and dissemination instructions. FBI, National Security Division, and Criminal Division officials attributed these portion marking errors to either human error or formatting issues. National Security Division and Criminal Division officials further stated that the marking errors were generally attributable to the National Security Division and Criminal Division having received unmarked source documents from other components. One of the documents reviewed by the OIG contained a footnote specifying that the document lacked portion markings because the source document was not properly marked. DOJ officials were mindful of the requirement that classified documents should contain portion markings, but were unaware that if a classified source document is not marked correctly the receiving agency must request a revised version of the document.

Missing or Incorrect Dissemination Control Markings – We noted instances where dissemination control markings were not always carried

over from source documents. FBI and DEA officials attributed these instances to human error and stated that the control markings should have been carried over to the derivatively classified documents. However, some of these instances occurred when information from Intelligence Community documents was transferred to derivatively classified documents created by DOJ components that are not members of the Intelligence Community. National Security Division and Criminal Division officials stated that they were unaware of the requirements for the various dissemination control markings because they did not have access to or were unaware of Intelligence Community control and handling marking requirements. In addition, we found that many of the officials relied on previous training or experience received from past employment when handling and marking classified material, even if that experience was acquired when there was different and now outdated classification guidance.

Missing Classification Banner - We found various documents that did not contain an overall classification marking banner. In most of these instances, FBI, National Security Division, and Criminal Division officials stated that this was human error.

Factors Contributing to Classification Deficiencies

As recognized in EO 13526, protecting information critical to national security and demonstrating a commitment to open government are accomplished through accurate and accountable application of classification standards, including uniform classification marking systems and security classification guides, as well as the use of technology needed to share national security information. As explained below, we found that the classification deficiencies identified during our audit were often attributable to the following factors: deficiencies in DOJ's implementation of classification and control marking guidance; inadequate and inconsistent use of security classification guides; a lack of automated tools capable of improving classification processes; deficiencies in the systems infrastructure used to process and store classified information; and weaknesses in DOJ's security education and training programs.

Classification and Control Marking Guidance

As previously mentioned, NARA issued the Information Security Oversight Office's *Marking Classified National Security Information* booklet to provide a baseline overview for classification marking requirements for original and derivative classifiers. In addition, ODNI issued the CAPCO Manual to provide members of the Intelligence Community with a standard set of classification marking requirements and instructions for using

agency-specific dissemination and handling control markings. However, some DEA and FBI officials from these Intelligence Community sections who were responsible for classifying the documents that the OIG reviewed were either unaware or only vaguely familiar with the CAPCO Manual. These officials instead relied upon prior knowledge and on-the-job training when marking classified documents.

In addition, DOJ officials from the National Security Division and Criminal Division work directly with the Intelligence Community to produce legal documents based on information obtained and classified by the Intelligence Community. However, DOJ officials from these divisions said that they were unaware of ODNI's policies and procedures regarding dissemination control markings as stated in the CAPCO Manual and used on documents provided by Intelligence Community agencies. These officials only referenced the Information Security Oversight Office's *Marking Classified National Security Information* booklet when derivatively classifying Intelligence Community information.

Of particular concern was National Security Division officials' lack of knowledge of the requirement for FISA markings in classified documents, as defined in the CAPCO Manual. Specifically, the CAPCO Manual contains a requirement that documents with FISA-obtained information contain a FISA-specific control marking. The National Security Division is responsible for overseeing implementation of FISA and receives numerous documents with such markings from agencies within the Intelligence Community. However, the National Security Division does not belong to the Intelligence Community, does not follow the CAPCO Manual guidelines, and does not use the FISA-specific markings. Moreover, National Security Division officials explained that when creating new classified documents they do not carry forward the FISA-specific markings from the original source documents from the Intelligence Community.

In September 2012, SEPS published the *DOJ Marking Classified National Security Information* guide, the first DOJ-specific marking guide ever produced. This marking guide is more comprehensive than the Information Security Oversight Office's *Marking Classified National Security Information* booklet. However, we found that DOJ's guide did not incorporate all Intelligence Community marking requirements. Therefore, we believe that SEPS should ensure that all DOJ components that work with Intelligence Community national security information – not just those components that are formally part of the Intelligence Community – have the necessary training to understand the marking and dissemination controls in the CAPCO Manual and to ensure that appropriate dissemination control markings are applied as required.

In addition, we believe that SEPS should improve the *DOJ Marking Classified National Security Information* guide to address the various ways to properly mark and classify e-mail correspondence and classified meeting notes. For example, the overview of how to mark a classified e-mail does not provide instruction for forwarding e-mails or how to elevate the classification of an e-mail if the response contains information at a higher classification than the original e-mail. Moreover, there is no overview of how to classify notes from in-person meetings or secure phone calls where national security information is discussed.

According to SEPS officials, the derivative classification concept and principles do not change because information is in an electronic format or because information is provided during in-person meetings and phone calls. However, as identified by the OIG during the audit, many individuals found that it was difficult to interpret classification and marking guidance and apply these instructions to e-mails and meeting notes. Further, although SEPS clearly indicated to the OIG that items such as meeting notes would be considered "working papers" and would not require classification marking due to their status as temporary documents, this is not noted in the guide. Therefore, we believe that SEPS and DOJ component Security Programs Managers need to ensure that personnel understand how to mark and classify all types of communication and documentation formats.

Therefore, we recommend that SEPS review the *DOJ Marking Classified National Security Information* guide and incorporate comprehensive instruction for marking all types of classified products, including e-mail correspondence and meeting notes.

Security Classification Guide Use

As previously stated, security classification guides are instructions from OCA officials on how to properly classify information. None of the National Security Division or Criminal Division classified documents reviewed by the OIG were derived from a security classification guide. Many officials that created these documents were unaware of how to use a security classification guide and did not know that DOJ had established the *DOJ National Security Information Security Classification Guide* for use by all DOJ components.

In addition, during our review of FBI classified documents, we found it difficult to determine if the classification decision was appropriate because the classification block did not convey enough information to identify the element within the *FBI National Security Information Security Classification*

Guide used as a reason for classification. When we asked FBI officials about their process for determining the classification of information, they informed us that they do not actually consult the *FBI National Security Information Security Classification Guide* when derivatively classifying documents. The reason the *FBI National Security Information Security Classification Guide* was identified as the source in the classification block was because selecting the *FBI National Security Information Security Classification Guide* as the source for all derivative classification decisions was a general practice.

We found that, in general, the DEA properly sourced its derivatively classified documents to the *DEA National Security Information Security Classification Guide* and identified the specific elements in the guide used to classify the information. The *DOJ National Security Information Security Classification Guide* states that when using one item in the security classification guide as the derivative source of classification, derivative classifiers should identify the item number within the classification block. However, the DOJ guide also states that when a derivative classifier uses multiple line items within the security classification guide to classify information, it is sufficient to only cite the security classification guide and not the specific line items. According to SEPS officials, the general cite should be used when there are four or more line items that apply to the classified information.

The use of security classification guides should facilitate the proper and uniform derivative classification of information. SEPS should ensure that all DOJ components understand how to properly use security classification guides to derivatively classify documents. Moreover, we believe that including specific line items is a good practice to ensure accountability for classifying information and also helps facilitates the review of classified information during the declassification process. Therefore, SEPS should reinforce to DOJ components its requirement for DOJ components to include the specific item number of the security classification guide used as the source of the derivative classification decision and clarify that this is necessary for up to four line items when multiple line items are used.

Automated Classification Marking Tools

During our review, we identified various automated tools used by DOJ components to mark classified information. Each automated tool provided DOJ components with a more efficient process for marking classified information and also provided these components with more assurance that classified information was properly marked.

For example, to help standardize and expedite the classification and marking of national security information, ODNI developed a Classification Management Toolkit (CMT) for use by members of the Intelligence Community. The CMT is an automated application that classifiers use to generate and apply classification markings to documents and e-mails, including a classification banner, classification block, and portion markings. Currently, the CMT is only available to the FBI and DEA for use on their classified networks because these two components are the only DOJ components within the Intelligence Community. The CMT is not available to any other DOJ components that work with classified information on JCON-S or JCON-TS, DOJ's Secret and Top Secret information sharing networks, respectively.

Officials from DOJ components without CMT installed on their systems informed us that they were interested in obtaining an automated system such as CMT. SEPS officials initially told us that DOJ was interested in acquiring CMT for all DOJ components, but funding was not available. However, in May 2013 SEPS began gathering information from the CMT Program Office within ODNI regarding the cost and requirements to determine CMT's functionality and the feasibility of installing it for use throughout DOJ.[32]

We observed the CMT's classification marking process and interviewed officials who used the CMT to classify their documents and e-mails. We believe that the CMT expedites the processing of classifying information and improves compliance with classification guidance by requiring derivative classifiers to include required classification markings on their classified documents. However, we also found that the use of CMT does not replace the need for oversight and training based on our finding, discussed above, that some derivatively classified FBI documents we reviewed contained marking errors, such as not including the identity of the classifier and referencing outdated source information, despite the fact that the derivative classifiers had used CMT to mark the document.

[32] According to an FBI official, the entire program cost of CMT is split between the 20 Intelligence Community "customers." When CMT was first installed, the FBI made an initial outlay of $16,000. According to FBI officials, the FBI has not incurred any costs for CMT since the initial outlay because ODNI has covered additional costs for maintenance and upgrades. However, an official at the FBI stated that although ODNI has covered subsequent costs for CMT, ODNI recommended that the FBI allocate additional resources for CMT just in case ODNI requires an FBI contribution in any given year and to cover any "FBI-specific" CMT modifications.

Another automated marking tool we encountered during the audit was an automated program based on commercially available technology to assist attorneys with drafting FISA applications. The program, developed by the Office of Intelligence at the National Security Division, automatically provides templates for regularly used documents, as well as a classification banner and document portion markings. This program has not been adapted for use by other sections within the National Security Division that develop other types of classified legal documents.

According to DOJ officials, these automated tools have helped to expedite and standardize the classification marking process for national security information. These tools have also assisted DOJ components in streamlining the process for creating standardized classified documents. We believe that all DOJ components that work with classified information could benefit from using automated classification tools to ensure that classified documents, in particular classified e-mail communications, are marked appropriately. We recommend that SEPS evaluate the possibility of using automated classification tools throughout DOJ.

Classification Protocols and Classified Infrastructure

DOJ components do not always have adequate infrastructure for accessing and sharing classified national security information. For many DOJ components, this adds a layer of complexity to working with classified information.

For example, an FBI official told us that sometimes the FBI and Central Intelligence Agency (CIA) will work with the same human source but may classify the information differently. Typically, the FBI will work with a source while he or she is in the United States and classify information from the source as either law enforcement sensitive or Secret, depending upon the subject matter. The CIA, in comparison, will work with the same source while he or she is overseas and classify information pertaining to the source as Secret//Sensitive Compartmented Information. Yet, when the agencies share their information with each other, the CIA's use of the additional Sensitive Compartmented Information caveat results in the FBI not being able to place the CIA's information on its regular classified system. Instead, the FBI must use an authorized Top Secret system or maintain the information in paper files. As a result, sharing the information with field offices or agents in remote locations can be arduous because not every FBI field office or satellite location has ready access to Top Secret systems. Therefore, to get this information to the proper personnel, the FBI must use other methods, such as requiring Special Agents to travel to another facility

to access an appropriate system, or relying on other government agencies to serve as a conduit for the information.

One information sharing tool is the use of "tearlines." Tearlines allow for the separation of pieces of information and enable the release of classified intelligence information with less restrictive dissemination controls, and, when possible, at a lower classification. The use of tearlines requires individuals to prepare a classified document in a manner such that information relating to intelligence sources and methods, or other highly classified information, is easily severable to protect such sources and methods from disclosure. We believe that in instances like the one described above, the use of tearlines would benefit DOJ components that do not have the proper infrastructure to access certain classified information.

However, the use of tearlines and similar workarounds is not a complete solution, as they do not solve the problem that DOJ does not currently have a comprehensive classified systems infrastructure capable of quickly and securely communicating highly classified or sensitive compartmented information to all personnel who may need to receive it. We therefore believe that SEPS should evaluate the current classified infrastructure in place throughout DOJ to determine what improvements are needed for DOJ components, in particular those DOJ components with field offices that work with Intelligence Community agencies, to successfully classify, use, and share all types of national security information. Moreover, we believe that DOJ components, especially the FBI and DEA, should convey to their Intelligence Community partners the need to provide classified information in a form that is as accessible as possible, consistent with the need to protect the information, and that they should consider the use of tearlines or other information sharing tools designed to increase information sharing wherever appropriate. SEPS officials stated that the Intelligence Community is evaluating tearline reporting and SEPS will convey to all DOJ components, through the Security Programs Managers, any guidance provided by the Intelligence Community.

Security Education and Training

During our interviews with DOJ personnel, many DOJ officials expressed a general lack of understanding on how to properly identify and mark classified information. DOJ personnel expressed significant confusion regarding the appropriate methods for identifying sources of classified information and marking e-mail correspondence and classified meeting notes. Many DOJ personnel also said that when they were uncertain about how or when to classify and mark information, they were more likely to err on the side of caution and mark the information as classified.

Moreover, few DOJ officials were aware of or used DOJ classification resources, including security classification and marking guides, when working with classified information. Instead, DOJ officials informed the OIG that they regularly relied on historical practices and prior knowledge to make classification decisions. In addition, officials explained that if they were unsure about how to classify and mark information, they would ask a colleague, who would have experience with the subject matter but may not have the expertise to answer a classification question accurately. We believe that this lack of understanding and reliance on "historic" processes resulted in many of the classification and marking errors we identified.

To correctly classify information, DOJ personnel need to receive comprehensive training that adequately prepares them to make informed classification decisions when dealing with national security information. DOJ personnel whose duties involve the creation or handling of classified information are required to take initial and annual refresher classification training that incorporates procedures for classifying and declassifying information. However, SEPS and some components within DOJ did not maintain a system that accurately tracked and verified whether individuals received and completed the required training. According to SEPS, many of the components reported in FY 2012 that original and derivative classifiers did not receive initial or annual refresher training. Moreover, many of the FBI, DEA, Criminal Division, and National Security Division officials we interviewed could not identify the training they received and suggested that a more robust training program would be helpful.

After reviewing DOJ components' training programs, as well as the training offered by SEPS, we found varying degrees of quality and depth. The FBI had the most comprehensive training program. The FBI offered ongoing instructor-led classification training sessions, as well as electronic training sessions that incorporated all aspects of the classification process and how to manage classified information. In comparison, we found that other DOJ components offered self-learning programs with no instructor-led portion. Further, some of these training programs did not provide an in-depth overview of the classification process, but rather focused on protecting and storing classified information. One of DOJ's OCA officials who received classification training through a slide-show format stated that he would have preferred a more interactive live training course because it would have provided him the opportunity to ask questions.

In FY 2013, SEPS officials recognized the need for training improvements and initiated automated slide-show training programs for DOJ components to use for their original and derivative classifiers. According to

SEPS officials, these training programs incorporated knowledge tests that help to ensure that at least the most basic elements of classification procedures are understood before an original or derivative classifier receives credit. However, we found that these training programs did not incorporate all aspects of security and classification requirements. Of particular note was the absence of an explanation of DOJ's classification challenge process, which entitles authorized holders of information to challenge the classification status of the information when the holder, in good faith, believes that its classification status is improper. We found that many DOJ officials were unaware of DOJ's formal classification challenge process. When the OIG informed SEPS about this discrepancy, SEPS officials stated that information relating to classification challenges is detailed in the SPOM and individuals are responsible for reading the SPOM, educating themselves on the classification process, and asking questions of the DOJ component Security Programs Managers. Although we agree that individuals are responsible for knowing and understanding DOJ's security policies and procedures as detailed in the SPOM, we also understand that the SPOM is more than 100 pages long and individuals rely on training programs to instruct them on these procedures.

Another aspect of classification management that was missing from DOJ's training programs was the instruction about what personnel should do when a source document is either not marked or marked inappropriately. As previously mentioned, we found documents that DOJ officials knew were not marked properly, but these officials stated that they did not know how to handle improperly marked source documents.

Finally, federal regulations require agencies to emphasize the importance of sharing and classifying information so it can be used to maximum utility. However, the SEPS training programs do not emphasize the importance of ensuring that information is classified at the appropriate level and not over-classified. Throughout interviews conducted during this audit, the OIG found that DOJ personnel were more likely to "err on the side of caution" when it came to classifying information. When there was any doubt about whether information should be classified, various DOJ officials in several components stated that they would most likely classify the information to avoid the risk of accidently releasing classified national security information. These individuals did not express significant concern for the possibility of over-classifying information, and some of these individuals stated – incorrectly in our view – that there are no consequences for over-classifying information, but that the consequences for releasing classified materials can be significant.

We attributed many of the classification and marking issues we identified throughout our review to inadequate training. Specifically, we believe that the individuals responsible for the classification decisions and application of appropriate markings were not sufficiently aware of the appropriate requirements because the training available throughout DOJ did not provide its personnel with the comprehensive knowledge regarding classification policies, procedures, and requirements needed to operate an effective classification management system. According to SEPS officials, resource constraints have negatively impacted their ability to operate a robust security education and awareness training program. We recommend that SEPS work with DOJ components, specifically the Security Programs Managers, to enhance classification training programs to ensure that all personnel are aware of policies, procedures, and requirements for classifying national security information.

Classification of Otherwise Unclassified Information

DOJ has both national security and law enforcement responsibilities. During our review, we found that when the DEA develops intelligence reports for dissemination to the Intelligence Community it takes unclassified law enforcement sensitive information, sanitizes the information to exclude operational information and conceal sources and methods, and upgrades the classification of that information to Secret. Therefore, the same piece of information can exist as unclassified law enforcement sensitive information in a DEA case file and as classified information in a DEA intelligence report. A DEA official explained that this information must be classified when it is disseminated to the Intelligence Community because it always has a foreign nexus and any compromise of this type of information may affect the DEA's operations, sources, and relations with foreign services, and would be damaging to U.S. interests. In addition, this DEA official explained that the DEA's classification practice is also based on the mosaic theory of classification, where individual unclassified facts can add up to classified facts when looked at in the aggregate. For example, according to this DEA official the fact that operationally derived information is routed to the Intelligence Community can elevate the classification level, as it can reveal information on the scope of the DEA's operations in particular areas.

Although we understood the DEA's concerns regarding the sharing of information, we also believed that this practice could cause the over-classification of information. The OIG reviewed the DEA intelligence reports and questioned the classification of the information in these reports, as well as the DEA's overall practice of classifying law enforcement sensitive information when it is shared with the Intelligence Community. In response, a DEA official informed us that the DEA's policy was in-line with DOJ and

ODNI policies for classifying information. Nevertheless, the OIG also brought this classification practice to the attention of both SEPS and DOJ's Department Review Committee (DRC), which functions as DOJ's oversight entity in resolving issues related to the implementation of EO 13526, including those issues concerning over-classification. Both SEPS and the DRC upheld the classification status of the DEA's intelligence reports, as these entities agreed that the mosaic theory of classification applied to DEA intelligence reports when combined with the fact that the reports were being shared with the Intelligence Community. However, SEPS and DEA officials acknowledged that certain portions within the classified intelligence reports were classified incorrectly.

Recommendations

We recommend that SEPS:

1. Explain to DOJ components the importance of reducing the number of OCA officials and have DOJ components re-examine their number of OCA officials.

2. Review all DOJ security classification guides and work with Security Programs Managers and OCA officials to identify and reduce redundancies and to ensure that instructions are clear, precise, consistent, and provide derivative classifiers with sufficient information to make accurate classification decisions.

3. Work with DOJ component Security Programs Managers to ensure that OCA officials understand the difference between original and derivative classification decisions and properly mark classified information according to the proper requirements of the classification decisions.

4. Ensure that ODNI's ORCON-specific training is promulgated to DOJ components once it is issued and coordinate with the DEA Security Programs Manager and officials representing all DEA entities using the ORCON control markings to ensure that DEA's use of dissemination control markings is appropriate.

5. Ensure that all DOJ components are aware of and understand how to apply classification resources and markings, in particular, security classification guides, the CAPCO manual, and required FISA-specific dissemination controls, as appropriate.

6. Review the *DOJ Marking Classified National Security Information* guide and incorporate comprehensive instruction for marking all types of classified products, including e-mail correspondence and meeting notes.

7. Reinforce to DOJ components its requirement to include the specific item number of the security classification guide used as the source of the derivative classification decision and clarify that this is necessary for up to four line items when multiple line items are used.

8. Evaluate the possibility of using automated classification tools throughout DOJ.

9. Determine what classified infrastructure enhancements are needed for DOJ components, in particular those DOJ components with field offices that work with Intelligence Community agencies, to successfully use and share appropriate types of classified information.

10. Work with DOJ components to enhance classification training programs to ensure that all personnel are aware of policies, procedures, and requirements for classifying national security information.

II. DOJ CLASSIFICATION OVERSIGHT AND MANAGEMENT

SEPS is responsible for managing and developing DOJ policy for classified national security information. SEPS has developed oversight and review processes for classified national security information, as directed by EO 13526, but has not successfully implemented those processes because of insufficient resources, deficient oversight, and inadequate assistance from DOJ components. For example, SEPS has developed a mechanism for collecting information regarding classification decisions by DOJ components and has executed a self-inspection program throughout DOJ. However, we found that DOJ components provided incorrect information to SEPS because they were uncertain of all reporting requirements.

SEPS Classification Management and Oversight

As the designated DOJ Department Security Officer, the Director of SEPS is responsible for managing and developing the policy for DOJ's classified national security information and ensuring DOJ's organizational compliance with classification laws, regulations, and directives, as appropriate. To accomplish this task, SEPS has promulgated the Security Program Operating Manual (SPOM), which provides the foundation for DOJ's security and classification management program.

With nearly 60,000 personnel authorized to potentially access and derivatively classify national security information, SEPS's responsibilities are significant. Previous reviews conducted in 2006 by the Government Accounting Office (GAO) and NARA's Information Security Oversight Office found that SEPS lacked adequate resources to implement DOJ's security classification program. During our audit, SEPS officials expressed concern that while EO 13526, the *Reducing Over-Classification Act*, and other mandates that are unrelated to classification have substantially increased SEPS's responsibilities over the past few years, SEPS has not received any additional resources to fulfill those obligations. These officials stated that the resource constraints necessarily limit the effectiveness of their oversight and management of DOJ's security and classification program.

SEPS's classification program activities do appear to be understaffed. SEPS has only one classification subject matter expert who, in addition to being responsible for overseeing the development and review of DOJ's security classification guides, is also responsible for the coordination and

development of DOJ's declassification guide and procedures.[33] Additionally, SEPS has only staffed a single 4-person team responsible for conducting on-site compliance reviews of DOJ's 3,500 facilities and 115,000 employees to ensure compliance with DOJ security policies and classification practices. Moreover, these compliance reviews do not focus exclusively on classification and marking procedures, but also include evaluations of physical, personnel, contractor, and document security; information technology; communications and operations; occupant emergency; continuity of operations; and safety and health programs.

Due to a lack of in-house resources, SEPS relies heavily on each component's designated Security Programs Manager, who oversees the component's internal security review programs and manages the associated security processes. According to SEPS officials, however, many Security Programs Managers do not have the appropriate background to manage the breadth of their component's security programs. These SEPS officials told us that some DOJ components assign the Security Programs Manager function to personnel as a collateral responsibility and do not devote adequate resources to train them on proper classification procedures. Some SEPS officials told us that these problems result in a high turnover rate for Security Programs Managers, which makes it difficult for SEPS to effectively coordinate and oversee the implementation of security policies and procedures.

During our review we found weaknesses in SEPS's execution of classification management requirements, including oversight of classified information and special access programs, classification reporting requirements, annual self-inspection reports, oversight of compromises to classified information, and implementation of regulatory requirements. Moreover, we identified that SEPS did not fully implement certain classification program requirements in accordance with EO 13526. We believe that some, but not all of these weaknesses resulted from or were exacerbated by resource constraints at SEPS.

Special Access Programs

Another weakness that the OIG found involved DOJ components participating in Special Access Programs (SAP) unbeknownst to SEPS. A SAP is a program established for a specific class of classified information and

[33] *United States Department of Justice Automatic Declassification Guide*, November 2012.

designed to impose safeguarding requirements that exceed those normally required for information at the same classification level.

During the course of our review, we found that the FBI was participating in an Intelligence Community SAP since 1999 and the DEA was participating in an Intelligence Community SAP with read-on procedures since 1991.[34] SEPS officials explained that both of these programs fall under the purview of the Intelligence Community and SEPS does not have any additional required oversight over these programs. However, SEPS officials also stated that as the entity responsible for ensuring DOJ's compliance with classification management procedures, SEPS should ideally be aware of all SAP programs that DOJ components operate, even if those programs fall under the auspices of the Intelligence Community. Therefore, in order to ensure that SEPS has a comprehensive understanding over DOJ's classification management program, we recommend that SEPS establish a policy for DOJ components to alert SEPS to its participation in SAPs that are overseen by the Intelligence Community.

Classification Program Reporting Requirements

SEPS annually prepares and submits to NARA's Information Security Oversight Office certain metrics on the number of DOJ classification decisions, number of challenges to DOJ classification decisions, DOJ classification training, and the associated costs of maintaining DOJ classified information. SEPS relies on the components to self-report the above information. Yet we found that although SEPS has collected this information as required, it has not verified the accuracy of the information reported even though some of the information submitted by components was questionable.[35] SEPS officials believe that Security Programs Managers must ensure that these reports contain accurate and reliable information before they submit them to SEPS. However, we found that DOJ components did not receive enough guidance on how to report the number of classified

[34] When an OCA official(s) determines that certain classified information requires additional safeguarding, agencies will implement "read-on" procedures to limit the number of persons with access to the information and control dissemination of the information.

[35] In FY 2012, the Criminal Division reported to SEPS that two personnel from one section generated 185 classification decisions through e-mail. However, when we requested a listing of the classification decisions, an official within the section said that she included all classified e-mail in the total derivative classification decisions – regardless of whether she was the originator of the initial e-mail. This official was unaware that only the initial e-mail in a string of e-mails should be counted as a classification decision. As a result, this official said that the majority of the derivative classification decisions that were reported to SEPS were reported in error.

decisions. Some component officials acknowledged that for FY 2012 they reported an incorrect number of classified decisions because they were unclear about the reporting requirements.

Self-Inspections

As required by EO 13526, in 2011 SEPS established a self-inspection program to help oversee DOJ's classified national security information program. To implement the DOJ self-inspection program, SEPS provided a self-inspection checklist that required DOJ components to evaluate adherence to classification principles and compliance with requirements covering original classification, derivative classification, declassification, safeguarding national security information, security violations, security education and training, and management and oversight. The self-inspections also require DOJ components to conduct annual reviews of their relevant security directives and instructions, examine a representative sample of their original and derivative classification decisions, and interview producers and users of classified information. Since FY 2011, SEPS has reported the results of the self-inspection program to NARA's Information Security Oversight Office.

We reviewed a sample of DOJ components' self-inspection reports and identified significant methodological errors. Some components reported that they had performed a review of classified documents, but the review procedure described in the report only entailed physical security reviews of offices and facilities and did not mention any type of document review. The OIG verified with some Security Programs Managers that they only conducted informal reviews that did not evaluate the classification and marking of documents. In addition, we found that some components did not conduct annual reviews, as directed, but conducted reviews on a tri-annual basis. Moreover, some components did not answer all of the questions included in the self-inspection checklist, which could indicate that the self-inspection review was incomplete.

SEPS officials were aware of the incompleteness and inaccuracies found in the components' self-inspection's reports in FYs 2011 and 2012 when they were initially submitted, reviewed by SEPS officials, and consolidated into DOJ's report to NARA's Information Security Oversight Office. However, SEPS did not follow up with DOJ components at the time to ensure that these reports contained the most reliable information. According to SEPS officials, this was due to its resource constraints and that only one specialist oversees the self-inspections reporting process and that the responsibility is a collateral duty.

In March 2013, SEPS implemented monthly focus meetings for Security Programs Managers to assist in implementing classification policies and procedures, including the self-inspection requirement. SEPS officials believe that these meetings will improve the management of security matters in DOJ, including the accuracy and reliability of the self-inspection reports. We recommend that, in addition, SEPS should evaluate its oversight of the self-inspections process to ensure that DOJ improves the reliability of information in its reports to NARA's Information Security Oversight Office.

Oversight of Compromised Classified Information

As required by NARA's Information Security Oversight Office's Classified National Security Information directive, SEPS established procedures to conduct inquiries into any reported loss, possible compromise, or unauthorized disclosure of classified information. The DOJ SPOM requires that DOJ components must report all of these incidents to SEPS through the component-level Security Programs Manager. Despite this requirement, we identified a significant incident at the FBI that was not reported to SEPS.

According to FBI officials, in 2010 the FBI incorrectly entered Top Secret information from an Intelligence Community agency into a Secret-level FBI database used to track terrorist threats. The incident was identified when an FBI employee was informed by the Intelligence Community agency that certain information, when combined, was classified at the Top Secret level. As part of this review, in March 2013 the OIG learned of the incident followed up with the FBI to determine whether the classified information had been removed from the Secret database and whether the classified information might also have been inappropriately included in other FBI systems. FBI officials told us that they were not certain whether the information was included in other FBI systems. Ultimately, it was not until July 2013, approximately 3 years after the incident and after multiple inquiries by the OIG, that the FBI completed the removal of the information from other FBI systems.

Notably, we found that the FBI did not inform SEPS of the compromise. In August 2013, after the OIG inquired about why the FBI had not met its responsibility to notify SEPS of the incident, the FBI officials informed us that they would notify SEPS that month. According to the FBI, the FBI's inability to meet this specific requirement was the result of limited resources responsible for reporting incidents to SEPS, as well as the lack of an enhanced, automated, and standardized reporting system at the time of the incident. We believe that this discrepancy was also, in part, the result of the FBI's Security Programs Manager not following specific requirements, as

defined by SEPS, and this underscores the need for better oversight of classification procedures. Therefore, we recommend that SEPS review DOJ components' procedures for reporting compromises of classified information and reinforce to Security Programs Managers the importance of reporting compromises of classified information to SEPS. SEPS officials stated that in early 2014, SEPS will provide Security Programs Managers with more robust training in this area.

DOJ Implementation of Regulatory Requirements

As part of the oversight of DOJ's classification management program, SEPS is responsible for ensuring that policies and procedures comply with all regulations and federal requirements. Although DOJ established classification policies and procedures to ensure that information is classified and disseminated appropriately, we found some instances where DOJ did not adequately address the following requirements of EO 13526.

- The DOJ SPOM does not explicitly include a statement that all individuals are free from retribution for challenging the classification of information.

- The DOJ SPOM does not discuss the process of transferring ownership of classified information with a transfer of functions. Such a discussion would be relevant, for example, when DOJ closes an office that handles classified information, as it did in 2012 when it closed the National Drug Intelligence Center and transferred all classified information belonging to that office to another agency.

- Not all DOJ components incorporated classification management into performance plans and evaluations for OCA officials, derivative classifiers, and security programs officials.

- DOJ did not publish the updated Mandatory Declassification Review processes in the Federal Register.

In addition, we found that the DOJ SPOM was not updated in a timely manner to correspond with certain ongoing DOJ classification practices. Specifically, although SEPS drafted procedures relative to controls over a particular classified program, it had not finalized those procedures and added them to the DOJ SPOM.

In response to the weaknesses identified above, SEPS officials stated that Security Programs Managers were instructed through memorandum, as well as during the self-inspection process, to incorporate classification

management in performance plans for OCA officials, derivative classifiers, and security programs officials. In addition, SEPS officials stated that the process of transferring ownership of classified information with a transfer of functions is the responsibility of DOJ components' Records Management Divisions. Moreover, SEPS officials do not believe that this process is significant to DOJ's security programs or the overall classification management program. Nevertheless, EO 13526 and its implementing directive explicitly discuss the process for transferring information for agencies that cease to exist. Therefore, we believe that the SPOM should include this subject area and inform DOJ employees that, within DOJ, the procedures components are required to follow when transferring ownership of classified information are a records management function and direct the reader to additional reference material.

According to SEPS officials, it has limited resources dedicated to classification management. Therefore, we believe that certain tasks, such as timely updates and reviews of enacted policies and procedures, are not always highly prioritized by SEPS. Although these specific discrepancies may not directly attribute to the misclassification of information, we believe that it is important that SEPS ensure that DOJ is in compliance with all regulatory requirements.

Recommendations

We recommend that SEPS:

11. Establish a policy for DOJ components to alert SEPS to participation in SAPs that are overseen by the Intelligence Community.

12. Evaluate its oversight of the self-inspections process to ensure that DOJ improves the reliability of information in its reports to NARA's Information Security Oversight Office.

13. Review DOJ component's procedures for reporting compromises of classified information and reinforce to Security Programs Managers the importance of reporting compromises of classified information to SEPS.

14. Incorporate in the SPOM a reference to the procedures DOJ components are required to follow when transferring ownership of classified information.

STATEMENT ON INTERNAL CONTROLS

As required by *Government Auditing Standards*, we tested, as appropriate, internal controls significant within the context of our audit objectives. A deficiency in an internal control exists when the design or operation of a control does not allow management or employees, in the normal course of performing their assigned functions, to timely prevent or detect: (1) impairments to the effectiveness and efficiency of operations, (2) misstatements in financial or performance information, or (3) violations of laws and regulations. Our evaluation of internal controls for the Justice Management Division, FBI, DEA, National Security Division, Criminal Division, and USMS was not made for the purpose of providing assurance on the agencies' internal control structures as a whole. The management of these DOJ components is responsible for the establishment and maintenance of internal controls.

Through our audit testing, we identified internal controls deficiencies within SEPS's oversight of DOJ's classification management program. Based upon the audit work performed we believe that SEPS lacks the controls necessary to effectively oversee DOJ components' compliance with certain classification reporting requirements and their implementation of security classification procedures. These matters are discussed in detail in the Findings and Recommendations sections of our report.

Because we are not expressing an opinion on internal control structures as a whole for the Justice Management Division, FBI, DEA, National Security Division, Criminal Division, and USMS, this statement is intended solely for the information and use of DOJ components involved in this review. This restriction is not intended to limit the distribution of this report, which is a matter of public record.

STATEMENT ON COMPLIANCE WITH LAWS AND REGULATIONS

As required by the *Government Auditing Standards,* we tested, as appropriate given our audit scope and objectives, records, procedures, and practices, to obtain reasonable assurance that management for the Justice Management Division, FBI, DEA, Criminal Division, and National Security Division complied with federal laws and regulations, for which noncompliance, in our judgment, could have a material effect on the results of our audit. The management for these entities is responsible for ensuring compliance with applicable federal laws and regulations. In planning our audit, we identified the following laws and regulations that were significant within the context of the audit objectives:

- Public Law 111-258 (2010), *The Reducing Over-Classification Act*
- Executive Order 13526, *Classified National Security Information*, December 29, 2009
- 32 CFR Part 2001 and 2003 Part V *Classified National Security Information*; Final Rule (2010)

Our audit included examining, on a test basis, the auditees' compliance with the aforementioned laws and regulations that could have a material effect on these DOJ components' operations. We accomplished this task by reviewing classification policies, procedures, and practices; identifying and analyzing documentation related to classification management, including training programs and self-inspection reports; interviewing personnel who oversee classification programs and who are responsible for classifying information; and testing classified documents to ensure they comply with all classification requirements. We did not identify any issues that caused us to believe that the FBI, DEA, Criminal Division, and National Security Division were not in compliance with the aforementioned laws and regulations.

In general, the Justice Management Division was in compliance with these applicable laws and regulations. However, we found that the Justice Management Division did not fully implement certain requirements. DOJ did not comply with the EO 13526 requirement to include in its implementing policy – the Security Program Operating Manual (SPOM) – a statement that all individuals are free from retribution for challenging a document. In addition, EO 13526 directed agencies to include Mandatory Declassification Review processes in the Federal Register, which DOJ had not fulfilled at the time of the OIG's review because it did not publish the most up-to-date

Mandatory Declassification processes. Finally, the DOJ SPOM does not discuss the process of transferring ownership of classified information with a transfer of functions, as required by EO 13526. These issues are identified in the Findings and Recommendations sections of our report.

APPENDIX I

AUDIT OBJECTIVES, SCOPE, AND METHODOLOGY

Audit Objectives

As mandated by Congress, the DOJ OIG conducted an audit to evaluate policies and procedures implemented by DOJ for its classification management program. Specifically, P.L. 111–258 (2010), the *Reducing Over-Classification Act* required that:

> The Inspector General of each department or agency of the United States, with an officer or employee who is authorized to make original classifications, shall carry out no less than two evaluations of that department or agency or a component of the department or agency to: (1) assess whether applicable classification policies, procedures, rules, and regulations have been adopted, followed, and are effectively administered within such department, agency, or component; and (2) identify policies, procedures, rules, regulations, or management practices that may be contributing to persistent misclassification of material within such department, agency, or component.

Scope and Methodology

We conducted this congressionally mandated review in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

The *Reducing Over-Classification Act* directed that the Inspectors General consult with NARA's Information Security Oversight Office and each other throughout the evaluations and coordinate amongst themselves to ensure that the evaluations follow a consistent methodology for report comparison. Pursuant to this mandate, the ODNI Office of Inspector General along with the Department of Defense Inspector General coordinated and facilitated a working group to develop a standard evaluation guide that we used as a basis for our evaluation.

To accomplish our objectives, we conducted over 100 interviews with officials from the Justice Management Division, National Security Division, Criminal Division, FBI, DEA, and USMS located in and near

Washington, D.C., as well as at the FBI's Chicago and Washington field offices and the DEA's Chicago Division.

Our testing included selecting and reviewing a judgmental sample of 141 original and derivative classification decisions made by the National Security Division, Criminal Division, FBI, and DEA. We chose these DOJ components because their classification decisions comprised a substantial percentage of all classification decisions made by DOJ components with an OCA official in FY 2012. Our sample selection methodologies were designed to give us a broad exposure of different classification decisions. Furthermore, the selection methodologies were not designed with the intent of projecting our results to the populations from which the samples were selected.

In addition, although the OIG has an OCA official and reported derivative classification decisions during our audit period, we excluded the OIG from our review to avoid a conflict of interest. The exclusion of the OIG from our audit work did not affect the results of our audit because the OIG did not meet the classification decision threshold we established for selecting DOJ components to review.

Classified Document Universe

The following table identifies the different types of classified documents that the OIG reviewed. As shown, our review provided a broad exposure to the different types of classification decisions made by DOJ component officials.

Classified Documents Reviewed

Document Type	FBI	National Security Division	Criminal Division	DEA	Total
E-mail	1	0	6	0	**7**
Court Document	0	4	15	0	**19**
Memorandum	7	21	4	0	**32**
Congressional Report	3	1	0	0	**4**
FISA Application	0	4	0	0	**4**
Other Report	0	1	0	0	**1**
Intelligence Information Report	8	0	1	11	**20**
Investigative Leads	0	0	0	17	**17**
FBI Electronic Communication	37	0	0	0	**37**
Total Documents	**56**	**31**	**26**	**28**	**141**

Source: OIG Analysis of DOJ Components' Classified Documents

National Security Division – To identify a sample of classified documents, we requested from the National Security Division Security Programs Manager a breakdown of both originally and derivatively classified decisions by all National Security Division offices in FY 2012 to determine which National Security Division offices made the most classification decisions. The Security Programs Manager informed the OIG that the National Security Division's Counterterrorism Section, Counterespionage Section, and Office of Intelligence made the majority of the derivative and original classification decisions during FY 2012.

We requested that officials from the aforementioned offices provide the OIG with a list of classified decisions made during the last quarter of FY 2012. From these lists, we selected a judgmental sample of 11 originally classified decisions and 20 derivatively classified decisions that included Secret and Top Secret reports, FISA-related documents, and memoranda. We also interviewed National Security Division officials who were the classifiers or the managers of employees who classified the sample documents to identify reasons for classification or marking errors.

Criminal Division – To identify a sample of classified documents, we requested from the Criminal Division Security Programs Manager a breakdown of both originally and derivatively classified decisions by all Criminal Division offices in FY 2012. From the information provided, we identified that the Drug Intelligence Unit and the Human Rights and Special Protections Section made the majority of Criminal Division's original and derivative classification decisions during FY 2012.

We requested that officials from the Drug Intelligence Unit and the Human Rights and Special Protections Section provide the OIG with a list of classified decisions made during the last quarter of FY 2012. From these lists, we selected a judgmental sample of 10 originally classified documents and 16 derivatively classified documents that included Secret and Top Secret reports, court documents, e-mails, and memoranda. We also interviewed Criminal Division officials from the aforementioned offices who were the classifiers or the managers of employees who classified the sample documents to identify reasons for classification or marking errors.

Federal Bureau of Investigation – The FBI reported its derivatively classified decisions for FY 2012 were based on a statistical projection. The FBI's statistical projection was developed from a random sample method implemented to determine a reasonable estimate for the total number of derivative classifications that were made over the 1-year period. Because the universe was an estimated projection, there was no list of actual classified decisions from which to select a judgmental sample of documents.

To overcome the limitation of not having a universe to choose from, the OIG requested a list of operational areas that create the most classified decisions. The FBI informed the OIG that the Counterterrorism Division, Counterintelligence Division, Cyber Division, and the Weapons of Mass Destruction Division create the most classified decisions.

The OIG requested a list of all cases that were *open* in the four FBI operational areas during the last quarter of FY 2012 in Chicago, Illinois; Washington, D.C.; and FBI headquarters. The FBI provided a listing of cases that were *opened* during the last quarter of FY 2012 in the selected operational areas and locations. From this listing of cases *opened* during FY 2012, the OIG judgmentally selected a sample of cases for review. Although the number of cases that were *opened* during the period was significantly lower than the number of cases that were *open* during the period, the OIG determined that the number of cases opened during the period was of sufficient number from each division and location to provide a broad range of documents for review.

From the listing of cases selected for review, the OIG then requested a listing of the classified documents associated with each selected sample case. From the listing of documents, the OIG judgmentally selected classified documents to review.

The OIG requested an additional list of all Intelligence Information Reports prepared by the FBI's Directorate of Intelligence in the last quarter of FY 2012. From this list, the OIG judgmentally selected a sample of classified Intelligence Information Reports created by FBI officials in headquarters and field offices to review.

The OIG also requested a listing of all reports containing FBI-generated classified information that were issued to Congress during the last quarter of FY 2012. From this list, the OIG judgmentally selected a sample of Congressional reports to review.

Finally, the OIG reviewed FBI documents that had been referenced as source documents during reviews of other components. In total, the OIG reviewed 56 derivatively classified documents and interviewed over 25 individuals from these operational areas and offices. The classified documents we reviewed included reports, case file documents, Intelligence Information Reports, e-mails, and memoranda. These documents included Top Secret, Secret, and Confidential classified documents.

Drug Enforcement Administration – To identify a sample of classified documents, we requested from the DEA Office of Security Programs a universe of both originally and derivatively classified decisions by all DEA offices. From the universe provided, we identified that the Office of National Security Intelligence, the Special Operations Division, and the Office of Special Intelligence made the majority of DEA's original and derivative classification decisions during FY 2012.

We requested that officials from the aforementioned DEA offices provide the OIG with a list of classified decisions made during the last quarter of FY 2012. From these lists, we selected a judgmental sample of 4 originally classified documents that included Secret investigative leads and 24 derivatively classified documents that included Confidential and Secret intelligence information reports and other standard reports. We also interviewed DEA officials from these sections who were the classifiers or the managers of employees who classified the sample documents to identify reasons for classification or marking errors.

Testing Process

To evaluate original classified decisions we reviewed each decision to ensure it met the criteria as mandated by EO 13526, 32 CFR Part 2001 and 2003, the Information Security Oversight Office's *Marking Classified National Security Information* booklet, and for DOJ entities that were part of the Intelligence Community, the CAPCO Manual.

Testing of Classification Decisions

Original classification decisions are used only for previously unclassified information and should not be based on a prior classified decision as found in a source document or relevant security classified guide. When making derivative classification decisions, derivative classifiers must observe and respect the original classification decision and carry forward to any newly created document the pertinent classification markings from the source document(s) or the security classification guide. The derivative classification decisions must also include a classification block, a classification banner that reflects the highest classification level of the information contained in the document and appropriate dissemination controls found in the document, and each portion of the document shall be marked with the classification level and any dissemination controls from either source document(s) or a security classification guide.

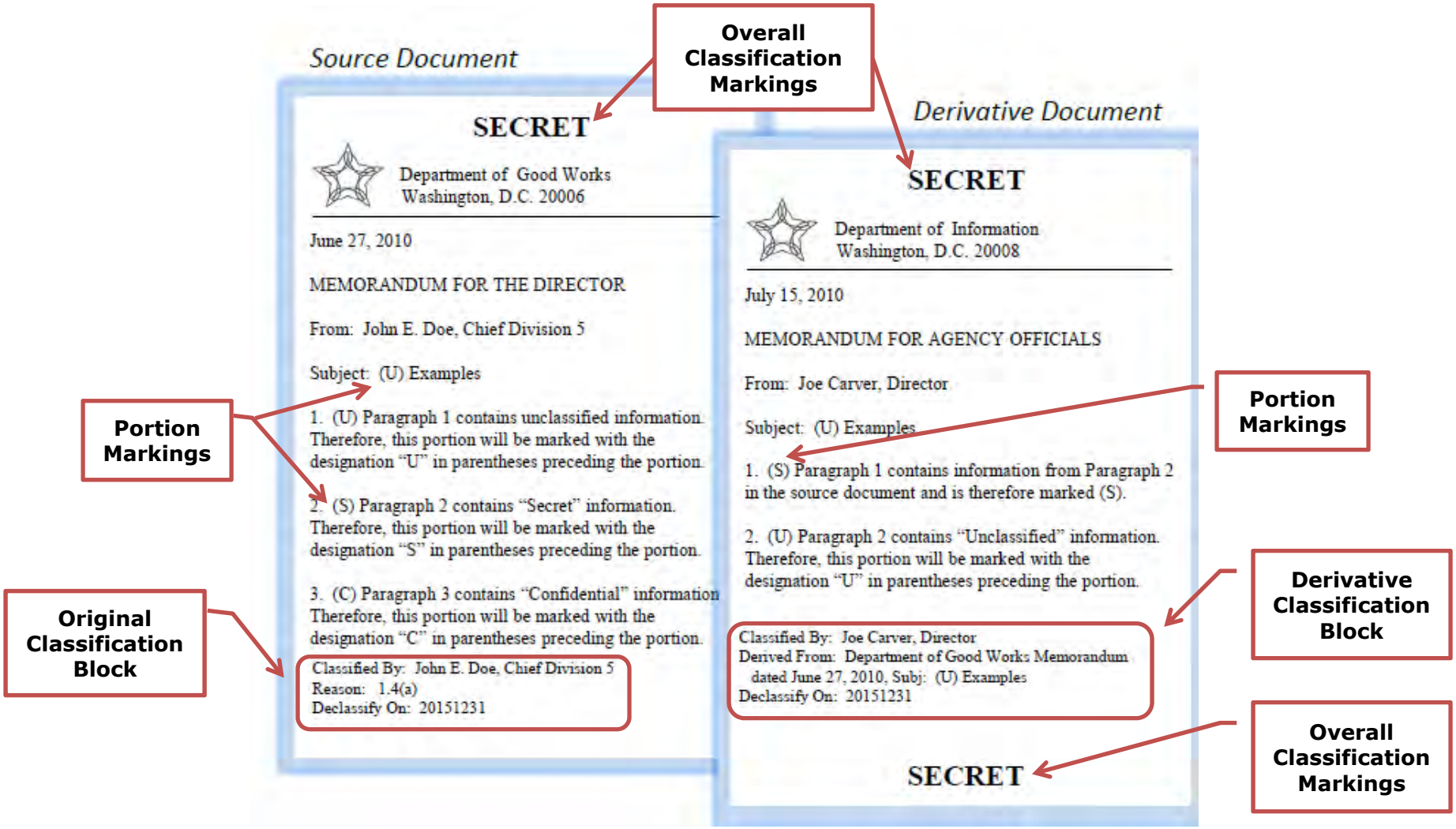
We reviewed a sample of DOJ original classification decisions to determine if these decisions were the first instance of classification and if the

classification reason provided was consistent with the EO 13526 requirements. As identified in the Findings and Recommendations sections of this report, we found discrepancies with the original classification decisions we reviewed.

In addition, we conducted a review of the classified information in the originally classified documents to assess whether it appeared to meet the level of classification assigned to it and if the reason assigned to it was accurate. Moreover, we reviewed the classified information in the derivative classification decisions to assess whether the classification level corresponded to the source documents and appeared to meet the level of classification assigned. In instances we identified as potential misclassification, we discussed our concerns with the classifier. In most of these instances the classification of information appeared to be justified, but as explained in the Findings and Recommendation sections of the report we identified a small number of documents that contained over-classified information.

Exhibit I-3 provides an overview of the classification marking requirements that the OIG evaluated for DOJ's original and derivative classification decisions. We reviewed DOJ classified documents to ensure that these markings were present and included all of this information and if the markings were appropriate for the information contained in the documents. For our evaluation of derivatively classified decisions, we ensured that the derivatively classified documents included the accurate and complete markings, as identified above. In addition, we reviewed these decisions to determine if dissemination and control markings were appropriately carried over from the source document(s) or security classification guide. As explained in the Findings and Recommendations sections, we found marking errors that we brought to the attention of DOJ officials.

CLASSIFIED DOCUMENT MARKING REQUIREMENTS



Source: NARA's Information Security Oversight Office, *Marking Classified National Security Information*, December 2010 (Revision January 1, 2012)

JUSTICE MANAGEMENT DIVISION'S RESPONSE TO THE DRAFT REPORT

U.S. Department of Justice

Washington, D.C. 20530

SEP 19 2013

MEMORANDUM FOR RAYMOND J. BEAUDET
ASSISTANT INSPECTOR GENERAL FOR AUDIT
OFFICE OF THE INSPECTOR GENERAL

FROM: Lee J. Lofthus
Assistant Attorney General
for Administration

SUBJECT: Audit of the Department of Justice's Implementation of National Security Information Classification Requirements

This responds to your September 9, 2013 memorandum requesting the agency's official response to the subject report. The sensitivity review and management representation letters will be provided under separate cover by the Department Security Officer. I appreciate this opportunity to provide comments on this report.

While the report sample did not find indications of widespread misclassification, I concur with the need to strengthen the Department's classification management program and ensure greater consistency in Department of Justice (DOJ) classification actions. Below are specific comments and proposed corrective actions to the recommendations.

1. **Explain to DOJ components the importance of reducing the number of Original Classification Authority (OCA) officials and have DOJ components re-examine their number of OCA officials.**

   Agree. The Security and Emergency Planning Staff (SEPS) will continue to work with individual components to ensure that their OCA delegations are evaluated according to the DOJ Security Program Operating Manual (SPOM). Section 4-102 (f) of the SPOM states that delegations of OCA shall be limited to the minimum required to administer Executive Order 13526, Classified National Security Information. In addition, Section 4-102 (h) states that components shall limit requests for OCA to those positions that have a demonstrable and continuing need to exercise this authority.

   To address this requirement, the Department Security Officer will notify all DOJ Security Programs Managers (SPMs) with delegated OCAs of the importance of reducing the number of OCAs, and instruct SPMs to re-examine their OCA delegations for possible reductions by October 4, 2013.

2. **Review all DOJ security classification guides and work with Security Programs Managers and OCA officials to identify and reduce redundancies to ensure that instructions are clear, precise, consistent, and provide derivative classifiers with sufficient information to make accurate classification decisions.**

   Agree. DOJ completed its first Fundamental Classification Guidance Review in July 2012. Per Executive Order 13526, fundamental classification guidance reviews will be conducted on a periodic basis thereafter, but shall be conducted at least once every five years. SEPS is currently working with the National Security Division (NSD) and the United States Marshals Services (USMS) to ensure that the DOJ National Security Information Security Classification Guide is updated and revised to adequately meet the requirements and needs of those components, to include providing clear, precise, and consistent information.

   In addition, SEPS will establish a Security Classification Guide Working Group which will include members from each component with delegated OCA. This working group will be established prior to November 15, 2013. The working group will review all DOJ security classification guides to ensure that security classification issues mentioned in this report are further identified and resolved in order to provide derivative classifiers throughout the Department with sufficient information to make accurate classification decisions. Updated and revised classification guides resulting from the efforts of the Security Classification Working Group will be disseminated to component SPMs and OCA officials by March 28, 2014.

3. **Work with DOJ component Security Programs Managers to ensure that OCA officials understand the difference between original and derivative classification decisions and properly mark classified information according to the proper requirements of the classification decisions.**

   Agree. SEPS will continue to work with component SPMs to ensure that OCA officials understand proper classification marking requirements and will further educate the OCAs regarding the difference between original and derivative classification decisions. In accordance with the SPM and Executive Order 13526, OCA officials are required to receive annual training on their OCA responsibilities, in addition to receiving annual classified National Security Information (NSI) refresher training, which includes classification marking requirements. The OCA and NSI refresher training are currently available on various DOJ learning platforms via computer based training. The difference between original and derivative classification is also detailed in the "DOJ Guide for Original Classification Authorities." The SPMs have been instructed to provide this guide to their OCAs.

SEPS will ensure that component OCAs have either completed the above training online or otherwise received training that meets the minimum standards of Executive Order 13526. Component SPMs with outstanding training requirements as of September 30, 2013, will be notified via email that they have until December 31, 2013 to ensure that their OCAs have received the appropriate training and that their OCAs understand the difference between original and derivative classification decisions. An acknowledgement statement will also be required by the OCAs stating that they understand original and derivative classification decisions and how to properly mark classified information according to the requirements of the classification decisions.

4. **Ensure that ODNI's ORCON-specific training is promulgated to DOJ components once it is issued and coordinate with the DEA Security Programs Manager and officials representing all DEA entities using the ORCON control marking to ensure that DEA's use of dissemination control markings is appropriate.**

Agree. Within DOJ, only the Federal Bureau of Investigation's (FBI) National Security Branch and the Drug Enforcement Agency (DEA) Office of National Security Intelligence are members of the Intelligence Community (IC), and are required to abide by ODNI guidelines and directives, in addition to those promulgated by the DOJ. These sections of the FBI and DEA, as members of the IC, are currently required by the ODNI to report on the use of ORCON as part of the annual reporting requirements outlined in Intelligence Community Directive (ICD) 710, Classification and Control Markings System. It is our understanding that the ODNI is currently developing training that will address the proper use, application, safeguarding, processes for dissemination, and derivative use of the ORCON marking. As IC members, this will be an ODNI directed mandatory training requirement for the FBI National Security Branch and the DEA Office of National Security Intelligence.

By October 4, 2013, SEPS will contact ODNI for an estimated training completion date. Once developed, SEPS will evaluate within 30 days of its completion the ODNI training, and will either choose to implement the training or work with the ODNI to develop within 90 days a similar version of the training that is appropriate to DOJ's general audience, including the DEA.

5. **Ensure that all DOJ components are aware of and understand how to apply classification resources and markings, in particular, security classification guides, the Controlled Access Program Coordination Office (CAPCO) manual, and required FISA-specific dissemination controls, as appropriate.**

Agree. SEPS will convene a security education working group consisting of component SPMs, no later than November 15, 2013 to evaluate training requirements, standards, and delivery methods. Training requirements and standards resulting from the efforts of this working group will be disseminated by March 28, 2014 to ensure DOJ components are aware of, and understand how to apply classification resources and markings.

6. **Review the DOJ Marking Classified National Security Information guide and incorporate comprehensive instruction for marking all types of classified products, including e-mail correspondence and meeting notes.**

   Agree. The purpose of the DOJ Marking Classified National Security Information Guide is to provide employees with an overview of their personal roles and responsibilities regarding information security. Specifically, it addresses what type of information can be classified, who makes classification decisions, and the proper markings to be used when classified information is contained in documents and media. The Guide was not developed, nor is intended to be, all inclusive. Rather, in instances where users of the Guide find it inadequate, they are advised to refer to the 32 C.F.R. Part 2001, and other Information Security Oversight Office (ISOO) issuances for further clarifications. SPMs are also to be consulted if users have questions.

   Although the Guide does currently contain guidance on email correspondence and meeting notes that conforms to and meets the requirements of marking guidance provided by the ISOO, by December 31, 2013, SEPS will expand upon guidance in those areas where this report has indicated a need for additional clarity.

7. **Reinforce to DOJ components its requirement to include the specific item number of the security classification guide used as the source of the derivative classification decision and clarify that this is necessary for up to four line items when multiple line items are used.**

   Agree. SEPS will revise the DOJ National Security Information Security Classification Guide and inform all components with classification guides currently in use of this identification requirement via email or in a meeting prior to December 31, 2013. SEPS will require components with classification guides to provide copies of this change and identify how this change was communicated to users of the guide.

8. **Evaluate the possibility of using automated classification tools throughout DOJ.**

   Agree. SEPS believes that an automated classification tool is greatly needed within the DOJ. As such, SEPS will continue to evaluate the possibility of using automated classification tools throughout DOJ. This is an ongoing and continuous process that involves DOJ Office of the Chief Information Officer (OCIO) and automated classification tool providers. SEPS will provide an evaluation on the feasibility of using automated classification tools throughout the DOJ by December 31, 2013. This evaluation will include expected costs and compatibility with existing systems.

9. **Determine what classified infrastructure enhancements are needed for DOJ components, in particular those DOJ components with field offices that work with Intelligence Community (IC) agencies, to successfully use and share appropriate types of classified information.**

   Agree. SEPS will continue to research best practices regarding classified document information sharing methodologies. Additionally, if and when the IC develops guidance designed to increase classified information sharing, SEPS will convey to all DOJ components, through the SPMs, the guidance provided by the IC. SEPS will also work with the DOJ OCIO to determine enhancements needed for an expedited and secure sharing of classified information via a comprehensive classified systems infrastructure. SEPS, in coordination with the OCIO, will provide a feasibility study by June 30, 2014, determining what classified enhancements are needed for DOJ components.

10. **Work with DOJ components to enhance classification training programs to ensure that all personnel are aware of policies, procedures, and requirements for classifying national security information.**

    Agree. This is a continuous process within the Department. As mentioned in Recommendation 5, SEPS will convene a security education working group no later than November 15, 2013 to evaluate training requirements, standards, and delivery methods.

11. **Establish a policy for DOJ components in the Intelligence Community to alert SEPS to the creation and operation of a SAP within DOJ.**

    Agree. SEPS is in the process of reviewing and revising Chapter 11 of the SPOM entitled "Special Access Programs." Once this review and revision is complete, the Department Security Officer will notify Department components of the reporting requirements pertaining to Special Access Programs. SEPS plans to have the policy revision and accompanying notification completed prior to March 28, 2014.

12. **Evaluate its oversight of the self-inspections process to ensure that DOJ provides reliable information in its reports to NARA's Information Security Oversight Office.**

    Agree. SEPS provided self-inspection training to the SPMs and component representatives in May 2013. The training included an overview of the self-inspection requirements and a thorough review of the self-inspection checklist. Self-inspection results and checklists from 2012 were provided to the SPMs in order to assist with the 2013 data call. SEPS conveyed its expectations for the components to coordinate with offices world-wide to obtain accurate data and to also develop internal self-inspection programs to be conducted semi-annually, at a minimum.

SEPS continues to work closely with component representatives throughout the ISOO self-inspection data call process to ensure accurate information is submitted. This is accomplished by detailed telephone calls, e-mails, and meetings with representatives addressing the checklist requirements. If the component believes the self-inspection program does not apply, SEPS coordinates with the appropriate officials to verify the validity in their response and further coordination and education is provided to the component if the program does apply. Each submission is also thoroughly reviewed and analyzed, taking into account the degree in which the component handles classified information.

For the 2013 self-inspection data call, SEPS will take the necessary steps to ensure all submissions are complete and accurate as possible. SEPS will thoroughly analyze each response and any areas of discrepancy will be validated with the submitting component. Additionally, component SPMs will be required to state that their submissions to the self-inspection data call are as accurate as possible to the best of their knowledge.

13. Review DOJ component's procedures for reporting compromises of classified information and reinforce to Security Programs Managers the importance of reporting compromises of classified information to SEPS.

Agree. The reporting of security incidents is reviewed by SEPS in coordination with the DOJ's Security Operations Center (JSOC). This process involves an automated e-mail notification from JSOC and a SEPS representative whenever a classified incident is reported by the components. Each incident is individually evaluated for further SEPS action.

An SPM training session for security incident reporting will be scheduled during FY 2014 and will reinforce the importance of reporting the compromise of classified information. Representatives of SEPS have individually met with the SPM staff for the FBI (most recently August 21, 2013), USMS (July 9, 2013), and ATF (July 18, 2013) to reinforce the importance of reporting compromises of classified information. Lastly, SEPS will draft a Department-wide instruction mandating incident reporting requirements to further reinforce the importance of reporting compromises of classified information. It is SEPS intent to have this instruction drafted by June 30, 2014, as this will involve in depth coordination with component SPMs and the DOJ OCIO.

14. Incorporate in the SPOM the procedures DOJ components are required to follow when transferring ownership of classified information and the requirements SEPS must use to ensure that components follow this protocol.

Agree. SEPS will update the SPOM or send out a policy memorandum to reflect language contained in 32 CFR Part 2001 by December 31, 2013. Transferring ownership of records, classified and unclassified is the responsibility of component records officers. 44 U.S.C. 2908 states that the Archivist of the United States shall promulgate regulations governing the transfer of records from the custody of one executive agency to that of another; and 36 CFR Part 1231 provides regulations that apply to records officers transferring records from the custody of one executive agency to another.

I am committed to a strong and effective classification management program, both in terms of improving our guidance and in terms of having DOJ components ensure their own classification actions are being correctly performed.

I appreciate the opportunity to comment on the report and convey the steps being taken to implement your recommendations. Should you have any questions or require additional information, please contact James L. Dunlap, Department Security Officer, at (202) 514-2094.

OFFICE OF THE INSPECTOR GENERAL ANALYSIS AND SUMMARY OF ACTIONS NECESSARY TO CLOSE THE REPORT

The OIG provided a draft of this audit report to the Justice Management Division (JMD). JMD's response is incorporated in Appendix III of this final report. The following provides the OIG analysis of the response and summary of actions necessary to close the report.

Recommendation Number:

1. **Resolved.** JMD concurred with our recommendation to explain to DOJ components the importance of reducing the number of Original Classification Authority (OCA) officials and have Department of Justice (DOJ) components re-examine their number of OCA officials. JMD stated in its response that the Security and Emergency Planning Staff (SEPS) will continue to work with DOJ components to ensure that OCA delegations are limited to the minimum necessary to administer Executive Order 13526, as required by the Security Program Operating Manual (SPOM). In addition, the Department Security Officer will notify all DOJ Security Programs Managers (with delegated OCA officials) of the importance of reducing the number of OCA officials and will instruct the components to re-examine their OCA delegations for possible reductions.

This recommendation can be closed when we receive evidence that SEPS has provided instruction to DOJ components on the importance of limiting their number of OCA officials and that DOJ components have re-examined their OCA delegations.

2. **Resolved.** JMD concurred with our recommendation to review all DOJ security classification guides and work with Security Programs Managers and OCA officials to identify and reduce redundancies to ensure that instructions are clear, precise, consistent, and provide derivative classifiers with sufficient information to make accurate classification decisions. JMD stated in its response that SEPS is currently working with the National Security Division and the United States Marshals Services (USMS) to ensure that the *DOJ National Security Information Security Classification Guide* is updated and revised to meet the requirements and needs of those components. In addition, JMD stated that SEPS will establish a Security Classification Guide Working Group to review and resolve issues in all DOJ security classification guides.

This recommendation can be closed when we receive evidence that SEPS has updated the *DOJ National Security Information Security Classification Guide* to include National Security Division and USMS classification requirements. In addition, please provide evidence that SEPS, in coordination with the Security Classification Guide Working Group, reviewed and resolved security classification guide issues, including redundancies and inconsistent instructions.

3. **Resolved.** JMD concurred with our recommendation to work with DOJ component Security Programs Managers to ensure that OCA officials understand the difference between original and derivative classification decisions and properly mark classified information according to the proper requirements of the classification decisions. In its response, JMD stated that OCA officials are required to receive annual National Security Information training and review the "DOJ Guide for Original Classification Authorities," both of which include information on classification marking requirements and the difference between original and derivative classification decisions. In addition, JMD stated that SEPS will ensure that DOJ OCA officials have completed the annual training requirements. JMD further stated that SEPS will require DOJ OCA officials to formally acknowledge that they understand the difference between original and derivative classification decisions and how to properly mark classified information.

This recommendation can be closed when we receive evidence that all OCA officials have received National Security Information training and have provided the acknowledgement that they understand the difference between original and derivative classification decisions and how to properly mark classified information.

4. **Resolved.** JMD concurred with our recommendation to ensure that Office of the Director of National Intelligence's (ODNI) Originator Controlled (ORCON) specific training is promulgated to DOJ components once it is issued and to coordinate with the Drug Enforcement Administration (DEA) Security Programs Manager and officials representing all DEA entities using the ORCON control markings to ensure that DEA's use of dissemination control markings is appropriate. In its response, JMD stated that as members of the Intelligence Community, the Federal Bureau of Investigation's (FBI) National Security Branch and DEA's Office of National Security Intelligence are required to report to ODNI on their use of ORCON. JMD further stated that ODNI is developing training that will address the proper use, application, safeguarding, dissemination process, and

derivative use of the ORCON marking. The FBI National Security Branch and the DEA Office of National Security Intelligence will be required to take this training. JMD further explained that once ODNI develops the ORCON marking training, SEPS will evaluate the training to determine if it will implement the training or coordinate with ODNI to develop more appropriate ORCON-specific training for DOJ's general audience, including the DEA.

This recommendation can be closed when we receive evidence that SEPS has either implemented ODNI's ORCON-specific training for DOJ components or developed a more appropriate ORCON-specific training for DOJ components. In addition, please provide evidence that SEPS has coordinated with the DEA Security Programs Manager and officials representing all DEA entities using the ORCON control markings to ensure that DEA's use of dissemination control markings is appropriate.

5. Resolved. JMD concurred with our recommendation to ensure that all DOJ components are aware of and understand how to apply classification resources and markings, in particular, security classification guides, the Controlled Access Program Coordination Office (CAPCO) manual, and required Foreign Intelligence Surveillance Act (FISA) specific dissemination controls, as appropriate. In its response, JMD stated that SEPS will establish a Security Education Working Group, comprised of DOJ component Security Programs Managers, to evaluate training requirements, standards, and delivery methods. JMD further stated that SEPS will disseminate the revised training requirements and standards to ensure DOJ components are aware of and understand how to apply classification resources and markings.

This recommendation can be closed when we receive evidence that SEPS has developed and disseminated to DOJ components training requirements and standards on how to apply classification resources and markings, in particular, security classification guides, the CAPCO manual, and required FISA-specific dissemination controls.

6. Resolved. JMD concurred with our recommendation to review the *DOJ Marking Classified National Security Information Guide* and incorporate comprehensive instruction for marking all types of classified products, including e-mail correspondence and meeting notes. In its response, JMD stated that the *DOJ Marking Classified National Security Information Guide* was not developed to be all inclusive. However, JMD stated that SEPS will expand upon the

guidance in the *DOJ Marking Classified National Security Information Guide* for marking classified e-mail correspondence and meeting notes.

This recommendation can be closed when we receive evidence that SEPS has provided comprehensive instruction for marking all types of classified products, including e-mail correspondence and meeting notes.

7. Resolved. JMD concurred with our recommendation to reinforce to DOJ components its requirement to include the specific item number of the security classification guide used as the source of the derivative classification decision and clarify that this is necessary for up to four line items when multiple line items are used. In its response, JMD stated that SEPS will revise the *DOJ National Security Information Security Classification Guide* and inform all components of this requirement. In addition, JMD stated that SEPS will require DOJ components with security classification guides to provide copies of this change and identify how this change was communicated to users of the component-specific security classification guides.

This recommendation can be closed when we receive evidence that SEPS has revised the *DOJ National Security Information Security Classification Guide* to include the item number identification requirement. In addition, please provide evidence that this requirement was included in all DOJ security classification guides and communicated to the users of those security classification guides.

8. Resolved. JMD concurred with our recommendation to evaluate the possibility of using automated classification tools throughout DOJ. JMD stated in its response that SEPS will coordinate with DOJ's Office of the Chief Information Officer and automated classification tool providers to evaluate the feasibility of using automated classification tools throughout DOJ.

This recommendation can be closed when we receive evidence that SEPS has conducted an evaluation on the feasibility of using automated classification tools throughout DOJ.

9. Resolved. JMD concurred with our recommendation to determine what classified infrastructure enhancements are needed for DOJ components, in particular those DOJ components with field offices that work with Intelligence Community agencies, to successfully use and share appropriate types of classified information. In its response, JMD stated that SEPS will research best practices regarding classified

document information sharing methodologies. Additionally, JMD stated that SEPS will work with DOJ's Office of the Chief Information Officer to determine enhancements needed for a comprehensive classified systems infrastructure to expedite the sharing of classified information. SEPS will provide a feasibility study regarding these enhancements.

This recommendation can be closed when we receive evidence that SEPS has identified and communicated to DOJ components classified information sharing best practices. In addition, please provide evidence that SEPS conducted an evaluation of DOJ's classified systems infrastructure to determine what enhancements are needed for DOJ components to successfully use and share appropriate types of classified information.

10. Resolved. JMD concurred with our recommendation to work with DOJ components to enhance classification training programs to ensure that all personnel are aware of policies, procedures, and requirements for classifying national security information. In its response, JMD stated that SEPS will establish a Security Education Working Group, comprised of Security Programs Managers from each DOJ component, to evaluate training requirements, standards, and delivery methods.

This recommendation can be closed when we receive evidence that SEPS has established the Security Education Working Group and enhanced classification training programs to ensure that all personnel are aware of policies, procedures, and requirements for classifying national security information.

11. Resolved. JMD concurred with our recommendation to establish a policy for DOJ components to alert SEPS to participation in Special Access Programs that are overseen by the Intelligence Community. In its response, JMD stated that SEPS will review and revise Chapter 11 of the SPOM entitled "Special Access Programs." In addition, JMD stated that once SEPS completes the revisions, the Department Security Officer will notify DOJ components of the reporting requirements pertaining to Special Access Programs.

This recommendation can be closed when we receive evidence that SEPS has revised the SPOM to include a policy for DOJ components to alert SEPS to participation in Special Access Programs that are overseen by the Intelligence Community. In addition, please provide evidence that the Department Security Officer has notified DOJ components of the new reporting requirements.

12. Resolved. JMD concurred with our recommendation to evaluate its oversight of the self-inspections process to ensure that DOJ improves the reliability of information in its reports to NARA's Information Security Oversight Office. In its response, JMD stated that in May 2013, SEPS provided self-inspection training to DOJ component representatives and Security Programs Managers. This training included an overview of the self-inspection requirements and a thorough review of the self-inspection checklist. In addition, JMD stated that SEPS will take the necessary steps to help ensure the validity and completeness of component-submitted self-inspection data. Moreover, JMD stated that SEPS will also require component Security Programs Managers to state that their submissions of self-inspection data are as accurate as possible.

This recommendation can be closed when we receive evidence that SEPS has conducted self-inspection training with DOJ component Security Program Managers and representatives. In addition, please provide evidence that SEPS conducted a thorough review of the FY 2013 self-inspection submissions and coordinated with DOJ components to verify the validity and completeness of the information.

13. Resolved. JMD concurred with our recommendation to review DOJ component's procedures for reporting compromises of classified information and reinforce to Security Programs Managers the importance of reporting compromises of classified information to SEPS. In its response, JMD stated that during July and August 2013, SEPS representatives met with security personnel at FBI, USMS, and the Bureau of Alcohol, Tobacco, Firearms and Explosives to reinforce the importance of reporting compromises of classified information. Moreover, JMD stated that during FY 2014, SEPS will conduct a training session for all DOJ Security Programs Managers to reinforce the importance of reporting the compromise of classified information. In addition, JMD stated that SEPS will coordinate with Security Programs Managers and the DOJ Office of the Chief Information Officer to issue a Department-wide instruction mandating incident reporting requirements.

This recommendation can be closed when we receive evidence that SEPS has reviewed DOJ components' procedures for reporting compromises of classified information and reinforced to Security Programs Managers the importance of reporting compromises of classified information to SEPS.

14. Resolved. JMD concurred with our recommendation to incorporate in the SPOM a reference to the procedures DOJ components are required to follow when transferring ownership of classified information. In its response, JMD stated that SEPS will update the SPOM or send out a policy memorandum to reflect language discussing the transferring of ownership of records language contained in 32 C.F.R. Part 2001.

This recommendation can be closed when we receive evidence that SEPS has either updated the SPOM or sent out a policy memorandum discussing the procedures for DOJ components to follow when transferring ownership of classified information.